DISTRIBUTION STATEMENT AUTHORIZATION RECORD

Title: Threats to Computer Systems

Authorizing Official: Jon Borden

Agency: DARPA Ph. No. 703-526-4166

☐ Internet Document: URL: _____
(DTIC-OCA Use Only)

Distribution Statement: (Authorized by the source above.) 8 MAR 13

☒ **A**: Approved for public release, distribution unlimited.

☐ **B**: U. S. Government agencies only. (Fill in reason and date applied). Other requests shall be referred to (Insert controlling office).

☐ **C**: U. S. Government agencies and their contractors. (Fill in reason and date applied). Other requests shall be referred to (Insert controlling office).

☐ **D**: DoD and DoD contractors only. (Fill in reason and date applied). Other requests shall be referred to (Insert controlling office).

☐ **E**: DoD components only. (Fill in reason and date applied). Other requests shall be referred to (Insert controlling office).

☐ **F**: Further dissemination only as directed by (Insert controlling DoD office and date), or higher authority.

☐ **X**: U. S. Government agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25.

NOTES: Mr. Borden, Enclosed is the document discussed per our telephone conversation in need of a distribution statement. Thank you for your assistance.

Joyce Keith (703) 767-9092 — DTIC Point of Contact

5 MARCH 2013 — Date

FINAL REPORT

UCRL-13574

THREATS TO COMPUTER SYSTEMS

Donn B. Parker, Stanford Research Institute

March 1973

Prepared under subcontract to:

The RISOS Project
Lawrence Livermore Laboratory
Contract No. AT(04-3)-115

Prepared for U.S. Atomic Energy Commission under contract No. W-7405-Eng-48

LAWRENCE LIVERMORE LABORATORY

University of California/Livermore

The RISOS Project is sponsored by the Advanced Research Projects Agency of the Department of Defense under ARPA Order No. 2166.

LAWRENCE LIVERMORE LABORATORY
University of California/Livermore, California/94550

UCRL-13574

THREATS TO COMPUTER SYSTEMS

by Donn B. Parker, Stanford Research Institute

MS. date: March 1973.

CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

PREFACE

As part of its continuing interest in the problem of how to improve computer security, the Advanced Research Projects Agency of the Department of Defense has funded a project, now under way at the University of California's Lawrence Livermore Laboratory, involving ways to measure, test, and evaluate the actual security of data stored in a computer system. This project, called RISOS (for Research in Secured Operating Systems), has, as its name indicates, a primary interest in finding out how operating systems can be made more secure. The focus of the project is on software security as opposed to physical security. Its goal is to develop detailed security guidelines that will be of value to both system design and system operation personnel.

One aspect of the RISOS project is that it will perform not only applied research but will also test and evaluate the security of selected computer systems, as specified by the Department of Defense. The orientation of these test efforts is one of close collaboration between RISOS personnel and the proprietors of host computers.

The largest representation of personnel in the RISOS group is systems programmers, but other disciplines are present as well. In addition to programming, systems analysis, and software research, the activities of the group include statistical analysis, modeling, and hardware analysis. The RISOS group is now in the process of developing and testing a series of special programs that will assist in assessing a system's limits and capabilities in order to obtain an idea of its security status. These testing programs have applicability to many types of systems in view of the amount of commonality that the group has observed between operating systems.

The survey effort embodied in this report has been of considerable use to the RISOS project in providing both a base of reference for investigating system security problems and a methodology for the study and analysis of future incidents.

--Robert P. Abbott
Principal Investigator
RISOS Project
Lawrence Livermore Laboratory
University of California
Livermore, California

FOREWORD

Computer-related crime[1] * is a term frequently used to describe the subject of this study. This impact term might be more accurately replaced by the following description: computer-related incidents of intentionally caused or threatened losses, injuries, and damage. This description covers the entire spectrum from crimes as defined by legislative action to unauthorized acts and disputed incidents. Such events will be referred to in this report as acts, cases, or incidents as applicable.

---

*Numbered references are listed at the end of the main body of the report.

I CONTRACT FULFILLMENT AND CONCLUSIONS

This report describes the results of interdisciplinary investigation and analysis of threats to the security of multiaccess, on-line computer systems and the development of a methodology for future similar investigations and analyses. The research was conducted in the Information Science Laboratory of SRI's Information Science and Engineering Division. The major activities included visits to computer manufacturers and computer service organizations; office and field investigation of incidents; attendance at conferences and a workshop; and meetings with the RISOS Project staff. One progress report, 11 visit reports, two oral presentations, two questionnaire case reports, and a case investigation manual were prepared and delivered to Project RISOS.

The reports on visits to computer manufacturers are included in the appendices and summarized in this report. The other reports on visits to MIT, Walpole Prison EDP Training Program, Tymshare, TRW systems, Credit Data, Rohr Industries, and Jerry Schneider (a computer crime perpetrator) are also included in the appendices.

A methodology that SRI developed for carrying out investigations is embodied in another document, Manual for Investigation of Computer-Related Incidents of Intentionally Caused Losses, Injuries, and Damage, and in the questionnaire designed to document cases for further analysis (see Appendix D). This methodology is based on experience in investigation of 46 of 129 reported cases over the past seven years. Two cases were investigated using the formalized methodology and are reported in questionnaire form (see the appendix of the investigation manual). A bibliography of 280 documents has also been separately transmitted to Project RISOS.

Interdisciplinary activity included consulting in design of the case investigation questionnaire with assistance from Dr. Brian Parker, Forensic Scientist; Mr. Steven Oüra, Research Sociologist; SRI legal council; and Dr. Peter Neumann and Mr. Carrol Kerns, Information Sciences.

This report includes a description and brief analysis of a case file of 129 cases of unauthorized acts involving computers, a summary of 19 cases involving multiaccess systems, a description of an empirical approach to threat analysis, and a detailed discussion of the nature of threats to computer systems. The report concludes with a summary report of the reaction and position of the computer manufacturing industry toward threats to computer systems.

The following conclusions were reached as a result of the research:

- Computer manufacturers claim incongruity between the federal and state governments on one hand, which demand security in standard computer products, and most commercial customers on the other hand who are unwilling to pay for such security.
- Demand for secure computer systems among commercial users will ultimately come about from legislation forcing security precautions and awareness of publicized, major computer-related crimes and the growing vulnerability of their organizations as they rely more heavily on electronic data processing (EDP). This demand is just starting to be noticeable.
- Security problems in multiaccess computers are rapidly approaching solution.[2,3] The remaining problems include positive personal identification from terminals, auditability and certification of computer security, metrics for the degree of computer security, cost-effective application of security features, and development of a body of knowledge of real breaches of computer security as an aid in optimally distributing security resources.
- Empirical threat models derived from actual experience are equal in importance to theoretically derived threat models in design and testing of secure computer systems.
- It appears feasible and practical to formalize the investigation methodology and analysis of unauthorized acts involving computers that result in damages, losses, and injuries. This formalization

will allow aggregation of data to validate threat models for use in developing and certifying the security of computer systems.

- The recording of 129 computer-related incidents, investigating many of them in varying degrees, and comparing the incidence and losses to the growth of computer usage indicate a significant new social problem.
- Conclusions from the case studies are applicable to computer security research and development:
  - Computer security should be developed on the basis that a penetrator of a computer system knows as much about the security features as the designers and implementors.
  - Security measures within a computer system at the present stage of development can be only as effective as the physical and personnel security surrounding the system.
  - Detection and effective reporting of anomalous activity within a computer system and its environment is equally as important as prevention of unauthorized acts.
  - All persons having access to a computer system should be aware of bounds within which they may operate and should be warned of possible sanctions for overstepping those bounds. The equivalent of NO TRESPASSING and DO NOT... signs should be visible to any user who exceeds or attempts to exceed security bounds in a system.
  - Unpredictable reasoning of unauthorized system penetrators precludes the effectiveness of assuming that a penetration work factor or bribe level of privileged system personnel greater than the worth of the assets protected is a measure of adequate security.
  - Monitoring the use of computers could be important for detecting the possible planning or practicing for attacks on computers.
  - A controlled access feature is of little value unless all attempted violations of it can be reported to the appropriate authorities in a timely manner for effective action.

- A significant increase in multiaccess system cases can be predicted on the basis of the proliferation of multiaccess systems containing, controlling, and processing valuable assets. The historic laissez-faire philosophy of computer users toward proprietariness of data, programs, and computer services and the user's image of the computer as an attractive subject of attack but not possessing personal attributes are factors that support this increase.

II EMPIRICAL APPROACH TO THREAT ANALYSIS

As with any area of research, a problem or challenge must exist to prompt such research. Research in security for computer systems used to be similar to nuclear reactor safety where few, if any, real disasters occurred, yet safety precautions had to be developed and made effective. Now, however, a small body of knowledge of reported cases of intentional acts against computer systems exists. The approach to computer security research need not be limited to theoretical considerations, penetration exercises, and well-circulated myths of computer crimes. There are enough real cases of unauthorized activities to support claims of increasing seriousness of the problem to justify accelerated security development efforts and enough real cases for analysis and conclusions about the threat. Real cases are superior to theoretical penetration exercises in some ways because they are occurring more frequently, they embody rational as well as unpredictable human behavior under natural stress, and they occur in real, undisturbed environments. Theoretical exercises are superior to real cases by being able to test specific security features under rigorous conditions in experimental systems. Therefore, both theoretical and empirical threat analysis is needed. Figure 1 illustrates how this process can be carried out in the overall research context.

Before proceeding to the next step of analyzing the nature of threats to computer systems and model development in Section V, the data base of case histories on which the analysis is based is described.

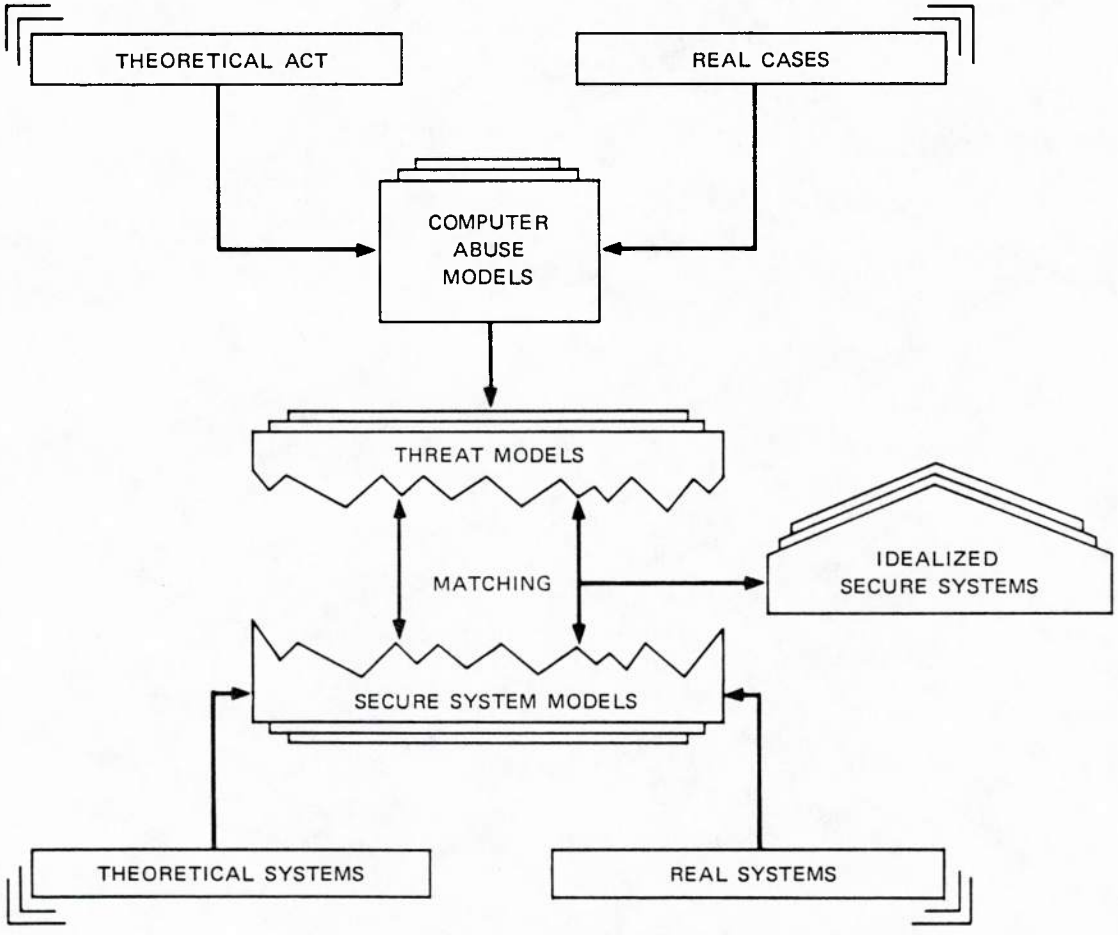

FIGURE 1 THREAT ANALYSIS METHODOLOGY

III UNAUTHORIZED ACT CASE HISTORY DATA BASE

The case file of unauthorized acts has increased to 129 reported incidents, with the addition of 38 since September 1972 when the project for RISOS started. (See Appendix F for summaries of new cases.) A total of 46 cases has been verified on the basis of direct contact, with one or more people involved or associated with each case. Several cases have been investigated in detail and documented in the appendix of the Investigation Manual.

Statistics drawn from the case file must be carefully qualified in reaching conclusions. Only 21 cases were privately reported; the remainder were discovered through news media stories, trade journal articles, talks, technical papers, and legal documents. Studies in criminology generally agree that about 15 percent of known cases of all types of crime are reported to law enforcement agencies. Applied to computer-related crimes, a file of 100 cases known and reported to police would imply that over 660 known cases are not reported to the police. Knowledgeable persons working in CPA firms indicate that a file of 129 cases covering a span of nine years represents only "a piece of the top of the iceberg of what's really going on." The assistant district attorney who prosecuted a recent case of program theft indicated that he has never encountered another profession in which so many unethical and potentially illegal practices abound.

A time-lag phenomenon occurs in reporting cases. This is evident in Figure 2 which shows a frequency distribution of incidents recorded when only 82 cases were known in April 1972 and now in March 1973 when

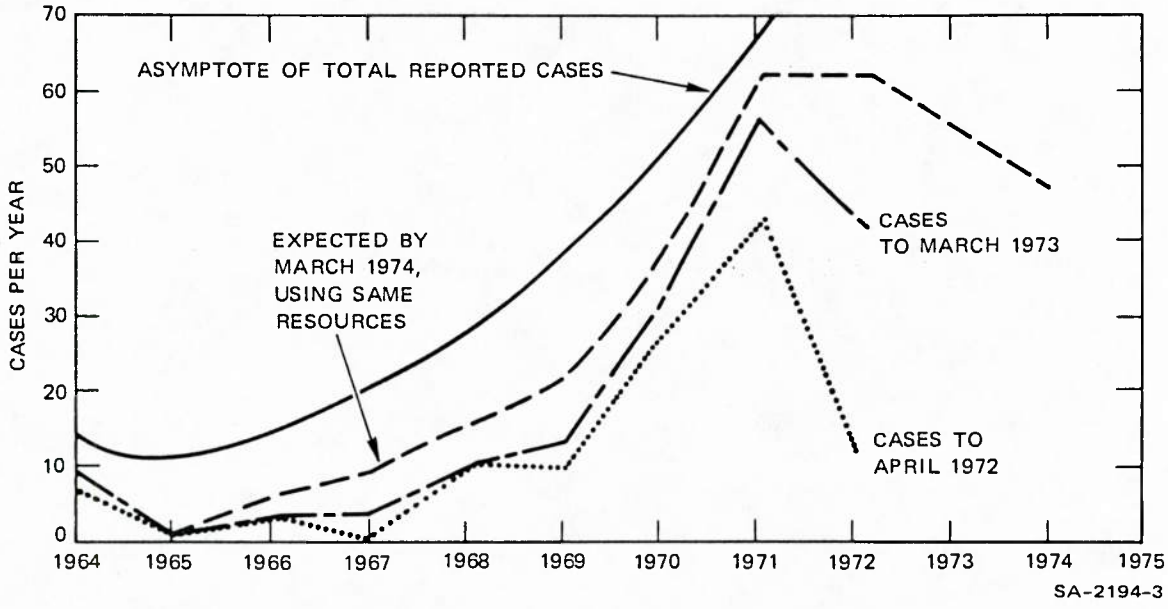

FIGURE 2 FREQUENCY DISTRIBUTION OF INCIDENTS

129 cases are recorded. It may be several years before a case is found or people are willing to reveal it.

Table 1 is a summary breakdown by year and by type of incident. Also shown are the number of verified cases. It is expected that counts for 1972 will soon exceed those of 1971 and, similarly, those of 1973. It must be realized that these numbers are also influenced by changing social conditions and attitudes that affect the willingness of victims to reveal their misfortune and of the public media to report them.

Computerworld weekly newspaper was the source of 48 of the 128 cases. The newspaper subscribes to several clipping services covering most newspapers for computer-related incidents and makes a practice of reporting most of them. An increasing number are being reported privately and directly to SRI as it becomes more widely known that the research project is collecting such information.

Table 1

CASES BY YEAR AND TYPE

(To Case 6924, 3/5/73)

	Vandalism	Information or Property Theft	Financial Fraud or Theft	Unauthorized Use or Sales of Services	Verified Cases	Total
1964		1	3		2	4
1965						
1966			1		1	1
1967				1		1
1968	1	1	4		1	6
1969	3	4	1		4	8
1970	7	5	6	5	11	23
1971	6	15	19	6	12	46
1972	5	14	9	8	13	36
1973	2	1	—	1	2	4
Total	24	41	43	21	46	129

It was assumed until recently that the United States is unique in proliferation of computer-related crime. However, 21 of the cases occurred in other countries, mostly in Western Europe. Unauthorized acts occur wherever computers are located.

It appears that no other organization is making an exhaustive attempt to collect, analyze, and report on computer-related crime data. The Internal Revenue Service has investigated a few of the more highly publicized cases. Dennie Van Tassel[4] at the University of California, Santa Cruz; Jerome Lobel,[5] a computer security consultant in Phoenix, Arizona; Brandt Allen,[6] University of Virginia; and Reiner von sur Muhlen,[7] a consultant in Bonn, West Germany, collect cases from newspaper stories and through personal experience with clients. Gerald McKnight, a professional author of Surrey, England, is writing a popular, nonfiction book on the subject.

Some valuable conclusions have already been reached in study of this limited data base, although they may change over the long term as a result of such factors as shifting social values, advancing computer technology and security methods, and proliferation of computers in bringing about the paperless society. The universal use of the questionnaire developed as part of this research (see Appendix D) to document and model each incident in the file will aid greatly in reaching additional conclusions and supporting findings from other sources. Data from the completed questionnaires can be used to provide frequency of occurrence of common factors and circumstances. Cross tabulation, multivariate and causal path analyses, and correlation of the data should reveal useful information. Some of the dimensions of statistical studies can include:

- Types of assets affected or threatened
- Location of such assets
- Purposes of the acts

- Positions of perpetrators of acts
- Background of perpetrators of acts
- Knowledge, skills, and access of perpetrators
- Types of access and entry to the computer
- Roles played by the computer and communications
- Types of computer systems and peripherals involved
- Types of software
- Types and extent of security subverted
- Methods of detection
- Methods of detection avoidance.

IV SUMMARY OF MULTIACCESS SYSTEM CASES

Reports of 19 cases of a total of 129 cases on file involved multiaccess computer systems. Two of the cases are thefts of entire operating systems and occurred in 1971. The remaining 17 occurred since 1969 and concerned terminal access using system commands. Five of these cases were limited to input/output manipulation of applications. Seven cases involved penetration of the operating systems. Four of the seven were to obtain unauthorized use of services; one was industrial espionage; another was vandalism; and the purpose of the last is undetermined. Five of the 19 cases occurred in university environments, the rest in businesses.

These 19 cases represent only 15 percent of the recorded cases. This is probably because of the small number of multiaccess systems compared with on-site batch systems in operation in the 1969-72 period. It is also caused by a time lag in discovering known incidents and a suspicion that more multiaccess system penetrations are not detected compared with the more obvious physical access usually associated with other types of systems.

The total number of cases and the number of multiaccess cases would be far higher if a methodical search were conducted among academic institutions. Although more unique and sophisticated methods would probably be discovered, less serious damage, loss, or injuries would be encountered than in business and government environments. However, there is a sinister potential to probable proliferation of the incidence of acts in an academic environment. Students rationalizing these acts as games and legitimate challenges with relatively benign results could produce a generation

of computer users in business and government with different ethical standards and great expertise in subverting computer systems. A study of cases in academic environments and a study of the attitudes and social values of students gaining such expertise is suggested and would be valuable in predicting the trends and nature of computer-related crime.

A significant increase in multiaccess system cases can be predicted on the basis of the proliferation of multiaccess systems containing, controlling, and processing valuable assets. The historic laissez-faire philosophy of computer users toward proprietariness of data, programs, and computer services and possibly the user's image of the computer as an attractive subject of attack but not possessing personal attributes are factors that support this increase.

Discussions with managers and systems programmers from computer time-sharing service companies, including four perpetrators of unauthorized acts, indicate that it is common practice to gain legitimate or unauthorized access to competitors' systems. Once gaining access, the perpetrators test the system's performance and features, take copies of programs and data files, test the security access control, and on penetration into privileged mode take private information and subvert the operating system making subsequent attacks simple. As a final act, they usually crash the system. In one example, the perpetrator was discovered by the victimized company and hired by the company to plug the holes he had found and made in the system. This young, bright systems programmer performed the penetration by adapting his knowledge and skill of his own company's system to the subject system. He rationalizes that this type of activity is not unethical or illegal and challenges anybody to prove that it is in the absence of legal precedence, contractual agreements limiting activity, or visible protective signs or warnings.

A trend of increasing incidence could be reversed by increasing the security of systems to a degree that only the most knowledgeable systems programmers associated with a system could penetrate it by establishing norms of professional conduct inhibiting such activities and by providing detection and warning features to confront an individual with the nature of his act and as a basis for legal action.

These data and conclusions are put into the context of the nature of threats to computer systems in the next section.

V MODELS OF THREATS TO COMPUTER SYSTEMS

Models are most effective in understanding the nature of threats to computer systems. These models can be used in the design and development of technological and social means to reduce the incidence and seriousness of the misuse of computers. Models of secure computer systems have become quite common.

Several threat models in varying degrees of detail and validation have been constructed. First, a parameterized model in the form of a questionnaire and checklist was constructed (see Appendix D) for use in the investigation of cases. An investigation methodology was developed and presented in a Manual for Investigation of Computer-Related Incidents of Intentionally Caused Losses, Injuries, and Damage. The appendix of the manual contains two completed questionnaires that represent parameterized models of two cases investigated in detail.

A conceptual model of the roles that computers play in incidents is described in Figure 3. A computer can be the subject of an incident. For example, several computer centers have been destroyed. Two thefts of small computers are known. In two cases, computers were shot with pistols by angry persons involuntarily and incorrectly served by computer applications.

Computers provide a unique environment in which acts occur. The uniqueness comes about in the new ways assets may be stored, processed, and transmitted. Computer programs represent entirely new types of assets created in this unique environment and subject to criminal and injurious acts. The largest number of 129 recorded cases fits into this category.

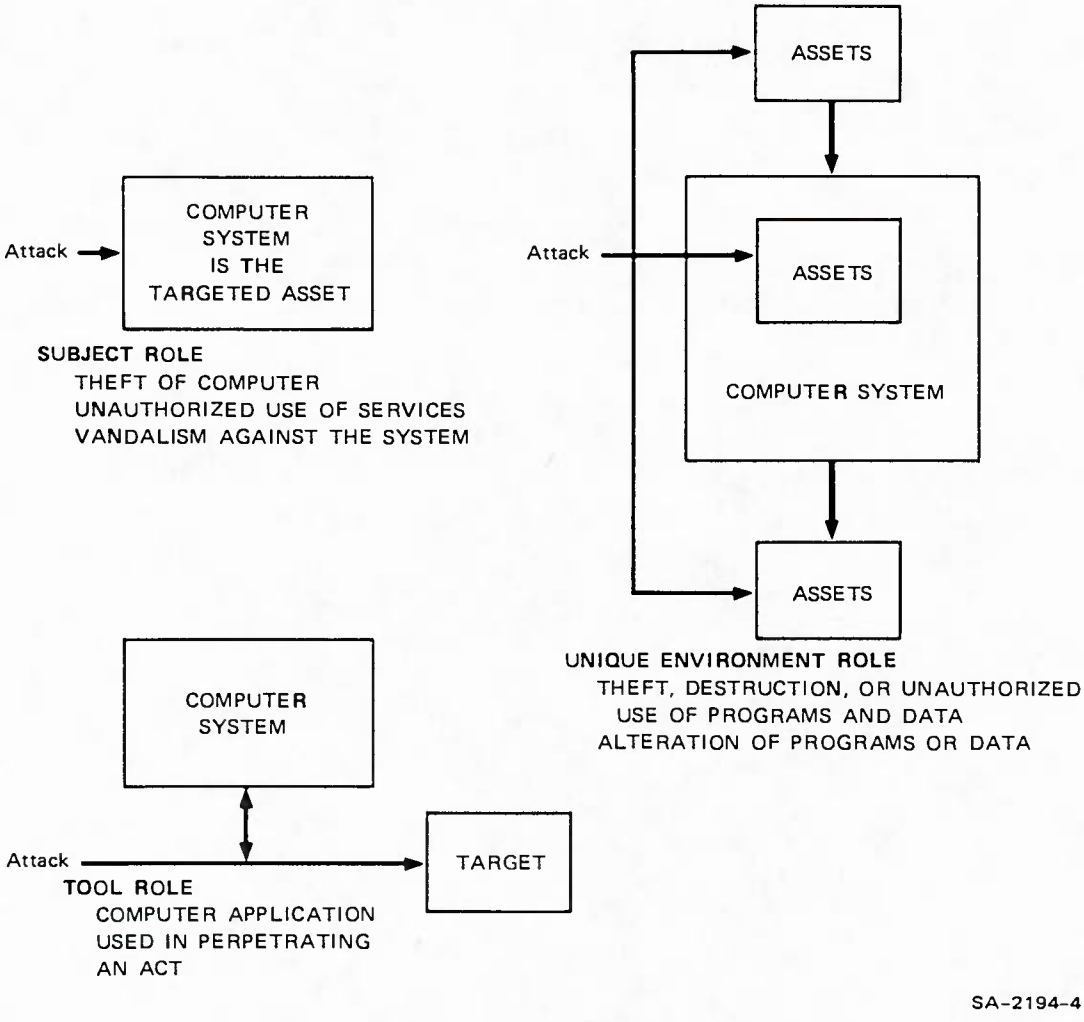

FIGURE 3 ROLES PLAYED BY COMPUTERS

Finally, computers can play the role of tools used to perpetrate acts. The acts need not be uniquely associated with computer technology, but the tool and often the methods are. In one case, a computer was used to regulate the rate and distribute among accounts the embezzlement of $1 million over six years. Computers can also be used to decipher password systems or encrypted information to penetrate other computers.

Among the three roles played, it is likely that a breakdown of the unique environment role into subroles appears most fruitful in further

understanding this subject. A study of the role of computers as tools in these acts indicates how important it is to a perpetrator to have access to a computer to develop the method of attack and to practice the attack to be made on a similar computer. This leads to the conclusion that monitoring the use of computers could be an important part of computer security in detecting possible planning or practicing of acts.

A sequential flow chart model as presented in Figure 4 can be a helpful device for understanding these acts. This model suggests that the attack (in box 6) may represent only a small part of an incident. Current computer security concentrates on this one aspect, probably because it is most amenable to technological solution. This model could be conceived as a threat model, and a comprehensive development of computer security should address each box in the diagram. For example, controlled access features in a computer system should be designed so that the appropriate witnesses (box 7) can and will observe attacks in a timely manner.

Box 9 ending without detection could mean less than successful results for some perpetrators. Several cases indicate the importance to some perpetrators of having the success of their efforts known. For some people, it would be frustrating to not be able to boast of a successful act. This is a significant aspect of the Jerry Schneider/PT&T case (see Appendix C). In a recent delayed-action computer penetration at Dartmouth University, the perpetrator had a complete confession stored as a file in the system he successfully attacked.

Another way to depict an incident is by a conceptual outline model, Table 2. It is divided into parts concerning perpetrators, subjects, and objects of the attack; planning; execution of the acts; detection; apprehension; sanctions; and recovery. This model provides a checklist for considering all aspects of an incident and is useful for devising

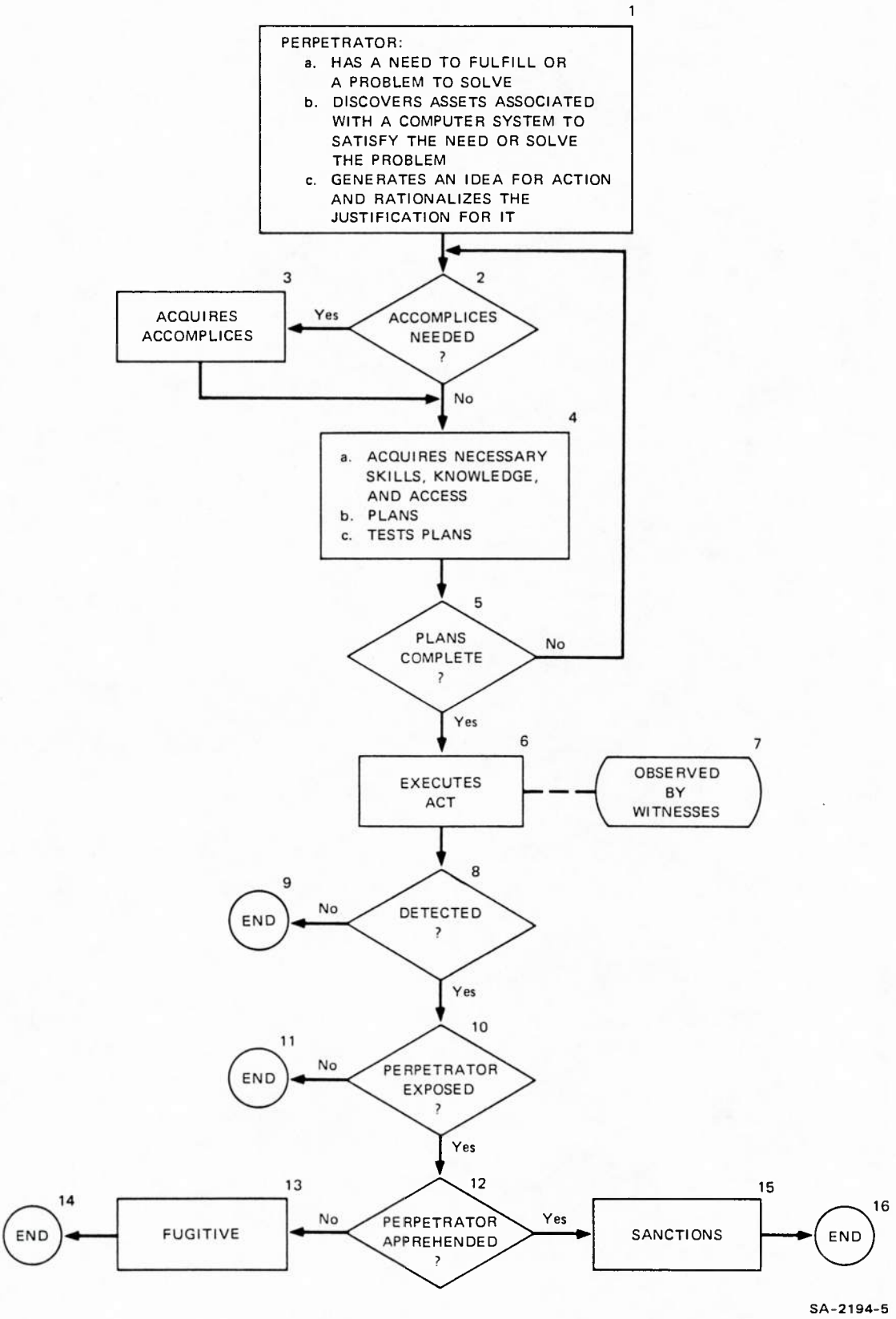

FIGURE 4 SEQUENTIAL FLOW DIAGRAM MODEL OF AN INCIDENT

Table 2

CONCEPTUAL OUTLINE MODEL OF AN INCIDENT

1. Perpetrators (1.*)
1.1 Skills and experience (4.2.4, 9, 10, 4.1.5, 3.5)
1.1.1 System use
2 Programming
3 Application usage
1.2 Knowledge (3.5.1)
1.2.1 Target system
2 Target applications
3 Target assets
4 Staff
5 Security features
1.3 Access (3.5)
1.3.1 Physical
2 Computer system
3 Privileged mode
1.4 Motivation (1.4.1, 2, 3)
1.4.1 Degree
1.4.2 Type
3 Financial gain
1.1.1.1 direct
2 Indirect
1.4.5 Positional gain
6 Ego gain
7 Challenge
8 Righting a wrong
9 Solving a problem
1.5 Accomplices (1.1.9)
1.5.1 Accomplice relationships
2 Accomplice motivation

2. Subjects and objects of the attack
2.1 Assets
2.1.1 Negotiable instruments
2 Credit (3.1)
3 Data (3.3.4, 3.2.1)
4 Programs (3.3.3, 3.2.4, 2.1.7)
5 Hardware (3.3.1, 3.2.4)
6 Materials (3.3.5)
7 Services (3.1)
2.2 Media (3.3.2)
2.2.1 Visible
2 Magnetic
3 Electronic
2.3 Location (2.1)
2.3.1 Computer (2.1.1)
2 Peripherals (2.1.2, 2.1.5)
3 Communication circuits (2.1.6)
4 Computer room (3.3.6)
5 Storage facilities (3.3.6)
6 Service facilities (3.3.6)
7 Personnel work areas (3.3.6)
8 Other
2.4 Protection (2.1.8-11)
2.1.1 Deterrence
2 Prevention
3 Secreting
4 Recovery
5 Detection

3. Planning (1.1.6)
3.1 Act rationalization
2 Rational impulsive approach
3 Target identification
4 Environment determination
5 Access (3.2)
3.5.1 Covert
2 Overt
3.6 Protection subversion
7 Timing
3.7.1 of the planning (1.1.10, 11)
2 of the act (1.5.1)
3.8 Action type (3.1)
3.8.1 Destruction
2 Acquisition
3 Acquisition of a copy
4 Transformation of assets to usable form
5 Alteration
6 Use
3.9 Collusion
10 Knowledge gain (4.4.7, 8)
11 Detection avoidance (3.4)
12 Anticipation of exposure
13 Disposition of assets

4. Execution of the acts (4.5.2)
4.1 Timing (4.5.1)
2 Plan deviations (4.5.6)
3 Circumstance deviations
4 Collusion (4.5.3)
5 Rational/impulsive actions
6 Multiple/single act
7 Errors (4.5.6)
8 Witnesses (1.5.4)

5. Detection of the acts and perpetrators (3.4.2)
5.1 By whom (3.4.3)
5.1.1 Victims
2 Perpetrators
3 Associates
4 EDP staff
5 Protection staff
6 Auditor
7 Other staff
8 Third party
5.2 Method (3.4.4)
5.2.1 Visual
2 Evidence analysis
5.3 When
5.3.1 Before
2 During
3 After
5.4 Reported to whom
5.4.1 Victims
2 Perpetrators
3 Attorneys
4 Insurance companies
5 Law enforcement
6 Court
7 Press
8 Others

6. Apprehension (3.4.2, 3)
6.1 Time
6.2 Confrontation
6.2.1 Private
2 Legal
6.3 By whom (3.4.3)
6.3.1 Victims
6.3.2 Perpetrators
3 Witnesses
4 Associate
5 EDP staff
6 Protection staff
7 Auditor
8 Other staff
9 Law officers
10 Insurance company
11 Others

7. Sanctions
7.1 By whom
Victims
Employer of perpetrators
Associates
Professional society
Government
Courts
7.2 Public Private
7.3 Type, amount (3.6)

8. Recovery of victims (3.7)
8.1 Recovery plan invoked
8.2 Degree of recovery

*The numbers in parenthesis are related section numbers for the questionnaire in Appendix D.

investigative approaches. For example, the questionnaire in Appendix D is related to this model by noting questionnaire section numbers following items in the outline model. Each major subject in the outline is discussed below.

Perpetrators--A profile of perpetrators is based on acquaintance with six known perpetrators and on technical writing in criminology by Cressey[8] and others.

Perpetrators are white-collar amateurs rather than emotional or professional criminals. Few women have been encountered, and when involved they tend to be accomplices employed as keypunch operators or clerks. Most perpetrators are 18 to 30 years old. A few of the embezzlers are older.

The best way to identify a potential population of perpetrators is on the basis of the unique skills, knowledge, and access associated with computer systems. These are the most important factors to consider in threats to computer systems. Professional criminals do not appear to have acquired the knowledge and skills yet (see the report on prison EDP training in Appendix B), and the effort required will limit the number of them relative to the probable number of skilled, manual criminals.

Designing security into computer systems assuming that perpetrators will not be aware of all the algorithms used is an exercise in futility. The principal threat against whom protection is required must be the penetrator who knows as much about the system as the designers do.

Motive is a less helpful means of identifying potential perpetrators. The challenge of penetrating systems is attractive to many programmers and has produced a small population of so called "system hackers" mostly in university environments. Most perpetrators have rationalized part or all of their acts. In fact, they often put more effort into rationalizing

their acts than in planning them (see the report on Jerry Schneider in Appendix C).

Perpetrators' acts often tend to deviate in only small ways from the accepted and common practices of their associates. In one case of program theft through a terminal, it was revealed in the trial that programmers in both the victim firm and perpetrator's firm were gaining access to each others' computers frequently. This is called the differential association theory by Sutherland,[9] the criminal psychologist who established the term, "white collar crime."

Another commonly found rationalization is the Robin Hood argument. Perpetrators tend to differentiate between doing harm to individual people, which is immoral, and doing harm to organizations, which they believe is not immoral. In fact, they often claim they are just getting even for the great harm organizations do to society. Jerry Schneider, one of the known perpetrators, said that he was motivated to perform his acts to make money, for the challenge of seeing how far he could go, and to get even with the telephone company which he believes does great harm to society.

It is concluded and strongly supported that perpetrators fear unanticipated detection and exposure. They tend to be highly motivated and amenable to meeting challenges. This makes detection as a means of protection at least as important as deterrence and prevention. Perpetrators tend to be amateur, white-collar criminal types for whom exposure of activities would cause great embarrassment and loss of prestige among their peers compared with professional criminals who are in a culture in which reactions are just the opposite.

Collusion is an important aspect of reported cases, occurring in at least 57 of 129 cases and seven of the 19 multiaccess system cases. Collusion is probably motivated by the differential association theory and

the need for different skills, knowledge, and access as a result of the complexities of computer technology.

Subjects and Objects of the Attack--The subjects and objects of attacks contribute to the uniqueness of computer-related crime. For example, as the cashless, checkless society approaches, financial crimes will entail transfers of credit rather than dealing with negotiable instruments. Magnetic and electronic media make assets more compact, easily and speedily transmittable, and potentially easier to protect and hide. Data and programs are more subject to theft by copying where the victim may not be denied continued use.

Computer programs represent a new asset subject to theft and theft by copying. The law frequently does not cover computer programs as subjects of theft. Theft law covers programs in Texas (Texas versus Hancock, 1968), but not necessarily in California (California versus Ward, 1972). The treatment of programs as properties is in transition relative to taxes, patents, and declaration of ownership. The ethics of using modifying, and taking others' programs is not clearly defined. Programs as property subject to theft will require further economic, political, and jurisprudential attention.

Time is an important aspect of assets. Computer time (usage) and its availability when needed constitute an important asset. The value of computer-related assets changes more rapidly than equivalent assets in manual systems.

New assets, their increased sensitivity to time, and new forms of assets in the new enrivonments of computer and communication systems clearly require new approaches in protecting them from new types of threats.

Planning--Planning an act can take great care and resources to be successful. Planning the penetration of a computer system is susceptible to failure because small changes in the software can cause large changes in penetration methods. A bug in a program to be used for attack can easily be fatal to a sophisticated act. Purposeful, minor changes in operating systems could be a useful security practice, although none of the reported cases indicate this yet.

The cases studied indicate that planning tends to be highly rational, not impulsive, and often requires expenditure of great time and resources. Jerry Schneider (see Appendix C) posed as a magazine writer, an employee, and a customer over a six-week period to become an expert on operating his victim's computer system.

Execution of Acts--There may be important legal questions as to what constitutes an act associated with computers. For example, does an act occur with the unauthorized changing of a program or each time the altered program is executed?

Delayed action methods can be complex. In one case, a Trojan Horse technique was used by imbedding instructions in an ordinary file maintenance utility program. These instructions performed a check of privilege level each time the program was used. Six months after the program was put into general use a computer operator ran the program at a sufficiently high privilege level to trigger the program to take over the operating system and establish a new resident, privileged program within the operating system that proceeded in turn to eliminate all the unauthorized instructions that produced it. Other cases have occurred where the acts are triggered by putting in dates and certain combinations of data or by occurrence of other events. These triggered actions occur when the perpetrator is in some relatively safe position to gain from the act and not be caught.

Detection of Acts and Perpetrators--Detection is an important aspect of protection of computer systems. As indicated earlier, perpetrators tend to greatly fear detection. Detection features within a computer system can be made difficult to subvert compared with prevention features that must be fixed in action and in fixed locations within the system to protect similarly located assets. Detection techniques, on the contrary, may be placed anywhere, can be easily moved, and parameters describing detection patterns and tolerances can be frequently changed to values unknown to potential perpetrators even though they may know the detection methods used. For example, three unauthorized attempts to use privileged system commands by a user within a specified time period may require more detailed monitoring of that user's activities and trigger an alarm at the operator's console to take precautionary actions. This level of monitoring may be too costly on a continuous basis. Therefore, it could be varied in frequency of application, number-of-attempt limits and time limits, thus keeping a potential penetrator off-balance unless he can subvert the detection feature or the person changing the parameter values.

Few among the reported and discovered cases were detected by those directly responsible for detection such as security officers or auditors. Discovery was usually accidental and resulted from the curiosity of programming, marketing, or operations staff about unusual activities. Below is a summary of detection that occurred in several cases.

Case	Detector	Detection Method or Reason
Unauthorized snooping in a time-shared system	Operator	Detected scratch tapes being read before written.
Time-delayed, Trojan Horse penetration of a time-shared system	Programmer	Noticed a foreign program in a dump of the operating system resident.
Theft of a program from a remote job entry system	Salesman	Noticed a proprietary program deck that had inadvertently been delivered by hand to a customer who had not requested it.

Case	Detector	Detection Method or Reason
Bank application program patched to avoid overdraft reports	Accountant	Noticed overdraft condition when manual processing replaced a computer that had failed.
Pension payment check fraud	Accountant	Noticed an unusual number of death notices of pensioners following the existence notice deadline.
Unauthorized sale of dossiers stored in a police system	Programmer	Placed a patch in the system to notify operator of a retrieval request for a specified name to trap the terminal user requesting it.
Unauthorized penetration of a time-sharing system	Operator, telephone company	Noticed an unusual number of crashes. Terminal used was traced by the telephone company.
Unauthorized use of time-sharing services	Operator	Noticed an unusual frequency of requests for game-playing programs.

Apprehension, Sanctions, and Recovery--These three sections of the model deal with subjects not of direct interest to RISOS and are included for completeness purposes only.

The reactions of potential victims of the threats described in this section are evaluated in the next section indirectly by considering the problems that computer manufacturers face in marketing security-oriented computer products.

VI REACTION AND CURRENT POSITION OF COMPUTER MANUFACTURERS TOWARD THREATS TO COMPUTER SECURITY

Computer manufacturers are gaining experience in developing new systems and modifying existing ones to incorporate security features; however, this is being done only for isolated, individual customers--mostly federal and state government agencies and several large banks and time-sharing firms. Otherwise, the manufacturers are caught between the demands of federal and state governments for security built into standard products and commercial customers' unwillingness to pay for security features.

Each computer manufacturer has one division or more with experience in developing secure features in computer systems; but in most companies the concern and experience do not pervade the commercial products divisions to any extent. Burroughs has a corporate staff man with part-time responsibility for security in products. Honeywell has a newly appointed staff headed by Jack Bremer in Phoenix concerned with standard product security; Control Data and Singer have no central responsibility; Univac has a committee as a focal point; and IBM has a full-time staff, headed by Robert Courtney in the Systems Development Division and Larry Foster leading a staff in the Federal Systems Division doing research, with the Resource Security System as a test vehicle.

The primary inhibiting factor is the lack of willingness of most customers to pay for security in the computer products they buy. Small segments of interested computer users have developed among bank credit reporting services and time-sharing services. Manufacturers also do not

see their customers creating secure physical facilities for their computers to match the degree of security possible in computers at even modest cost.

Another problem concerns the sensitivity of the secure state of an operating system to software changes. A manufacturer could produce an effective, controlled access system only to have the customers, continuing their common practice, modify the software and add other manufacturers' hardware, thus violating the integrity of the system. The inhibiting constraints and extra care required in updating a secure operating system precludes maintaining security in a computer system in today's typical computer facility environment. Several large time-sharing services are learning to maintain secure operating systems independent of the manufacturer, but it requires resources and a discipline beyond the means and motivation level in private, in-house computer facilities.

Secure features are gradually being incorporated into standard products at the level of preventing accidental or intentional incidents that result in losses, injuries, or damage. However, serious penetration attempts cannot be thwarted. Burroughs appears to be advanced at file access and sharing control at subfile (record or item) levels. Security is vested in the computer operator, and an extensive security monitor log is produced in the 6700 system. Honeywell's new 6180 Central Processor is advanced in integrated hardware and software security. Distributed authorization at the lowest user level is provided. IBM's newest OS releases are greatly improved in controlled access aspects. IBM provides extensive assistance to customers in the overall security of their facilities. Honeywell, Burroughs, and IBM have cryptographic hardware products in limited use and ready for general marketing when the demand arises. They also have made advances in methods of automatic identification at terminals that may result in products being available in 1973 for use in specialized applications such as point-of-sale transaction systems. All

manufacturers expect legislative actions over the next several years that will affect the secure computer system market.

Individual reports on visits with computer manufacturers are in Appendix A. Reports on visits to MIT, Tymshare Corporation, TRW Systems, TRW Credit Data, and Rohr Industries are in Appendix B.

REFERENCES

1. D. B. Parker, The Nature of Computer-Related Crime, Proc. International Conference on Computer Communications. ACM/IEEE (October 1972).

2. J. P. Anderson, Information Security in a MultiUser Computer Environment, Advances in Computers, Vol 12 (1972).

3. A. M. Noll, The Interaction of Computers and Privacy, Executive Office of the President. (Unpublished) February 12, 1973.

4. Dennie Van Tassel, Computer Crime, AFIPS Proc. Vol 37. FJCC, 1970.

5. Jerome Lobel, Privacy, Security, and the Data Bank, Government Data Systems (November 1970).

6. B. R. Allen, Computer Security, DPMA. Data Management (January 1972).

7. J. Turn and N. Shapiro, Privacy and Security in Databank Systems, AFIPS Proc. Vol 41. FJCC (1972).

8. D. R. Cressey, Other People's Money, a Study in the Social Psychology of Embezzlement, Wadsworth, Belmont, California (1971).

9. E. H. Sutherland, White Collar Crime, Dryden, New York, (1949).

Appendix A

REPORTS ON COMPUTER MANUFACTURERS VISITED

Appendix A

REPORTS ON COMPUTER MANUFACTURERS VISITED

SRI visited a number of computer manufacturers as partial fulfullment of its contract with the RISOS Project at Lawrence Livermore Laboratory. Donn B. Parker, project leader, reports on these visits in the following pages. Computer manufacturers visited, the persons contacted, and dates of the interviews are listed below.

Burroughs Corporation, Large Systems Division, City of Industry, California--Mr. Don Lyle, Manager of Programming Activity (8 February 1973).

Control Data Corporation, Minneapolis, Minnesota--Mr. Robert Morris, Director of Advanced Strategy (15 December 1972).

Digital Equipment Corporation, Maynard, Massachusetts--Mr. Kenneth Olson, President (5 January 1973).

Honeywell Information Systems, Inc., Wellesley Hills and Waltham, Massachusetts--Kurt Van Vlandren, Public Relations, Malcolm Smith, Education, Dr. John Weil, Vice President (11 January 1973).

Singer Business Machines Systems, San Leandro, California--Dr. Clair Miller, Software Development (19 January 1973).

UNIVAC Federal Systems Division, St. Paul, Minnesota--Frank Quirk (15 December 1972).

BURROUGHS CORPORATION, LARGE SYSTEMS DIVISION

This report concerns my interview with Don M. Lyle, Manager of Programming Activity in Burroughs Large Systems Division, who is responsible for all B6700 Computer system software. Mr. Lyle indicated that Edward Lohse in Detroit is the corporate staff person responsible for computer security. He also suggested that Dean Earnest, Lyle's counterpart at Burroughs' small systems plant in Goleta, California, would be interesting to talk with especially since he has extensive experience in cryptology.

Burroughs is working on a personal identification product that is secret at present but may be announced this year in conjunction with the Burroughs cash-issuing, stand-alone terminals. Lyle knows Doug Hogan at NSA and indicated that NSA has done some security-oriented testing of the B6700. Lyle noted the general reluctance of customers to pay for computer security except for some government agencies. He pointed out inconsistencies in security commitment by the computing community by indicating that no ANSI standards take security into account--for example, tape file labeling.

B6700 security features include memory protection, prohibiting users from using machine language, user identification and file access, and sharing authorization by name and password. After initial computer assignment of a password, a user specifies his own passwords. This has caused problems in reconstructing disk packs of files when disk failures occur. There is no mechanism to identify user-generated file passwords.

The B6700 has a WHO I command to return the serial number identification of the computer, but this feature is used only to hide new software features until they are ready for release to customers. All software sold or licensed by Burroughs is copyrighted and carries a copyright label, but no secret marking to identify software is done. Complete annotated listings of the system software, about 50,000 lines, are supplied to customers who frequently insert local changes and cause loss of any possible system security and integrity guarantees. System security is vested in the computer operator. Three monitoring logs of system activity are generated: a job log, hardware failure maintenance log, and a security log to record all anomalous activity associated with security matters such as LOGON failures. Only two attempts to LOGON are allowed before telephone disconnection is made. It is the customer's responsibility to do anything further with the logs.

A terminal-oriented file management and editing capability with extensive controlled access is provided. It allows sharing of files but only for reading or read/write. A new release will allow sharing and access control at the item level. The system maintains the creator of each file as the sole authorizing source. Lyle indicated it would take him about ten minutes of desk and terminal work to make unauthorized penetration of the system, but this capability requires detailed system knowledge possessed by only a few people.

Mr. Lyle described a computer-related crime that occurred in London. This is documented separately from this report.

CONTROL DATA CORPORATION

During my visit at Control Data Corporation in Minneapolis on December 15, 1972, I talked with the following people on the corporate staff: Robert Morris, Director of Advanced Strategy, Howard Squires reporting to Morris and responsible for computer security matters, David Jasper in Data Services under Robert Price and concerned with computer security, and a programmer responsible for 6000 Series file access methods.

Control Data is just starting to react to security needs. Those I talked with indicated no pattern of demands from customers for security in CDC products. They were unaware that the VIM users group has a committee on security and privacy (Tom Elrod of CDC attended a meeting of the committee, but I didn't talk with him.) CDC has a contract to develop software for a Swiss bank which includes significant protection requirements (RISOS should investigate this further).

Data Services is concerned about security. Jasper indicated that he was dealing with George Goode, President of Datotek, about possible use of Datotek cryptographic devices for telephone circuits. Jasper thought this product was the best on the commercial market. He acknowledged that the product was applicable only to point-to-point transmission and not to a multiplexed configuration.

Cybernet has a serious accounting problem that may tie in with a problem reported by RISOS personnel, although others disagree with Jasper and think it is not such a serious problem. Data Services provides its analysts with a privileged account number with no individual accounting of its use. Misuse by analysts to help a customer beyond what

company policy allows sometimes occurs. Large amounts of time are charged to this number occasionally (up to $10,000 worth per month). Data Services has not yet decided what to do. Employee turnover and possible misuse of information by ex-employees is another significant problem.

Jasper indicated that in the CEIR segment of the CDC, valuable LP programs are kept on tapes in a form writable and readable only by special I/O programs that put and contend with large numbers of parity and other errors, making them extremely difficult to read by standard I/O programs. Control Data disperses coded identification data throughout its software packages offered for sale or lease.

It is Control Data policy that security is its customers' problem unless otherwise handled by special contract. Hooks are placed in standard product operating systems for customers who wish to add their own access control. Hardware features exclusively for security purposes are not made standard parts of products because not all customers are willing to pay for them.

Bob Morris is responsible for developing means of monitoring computer products delivered behind the Iron Curtain to assure intended types of usage only as stipulated in federally approved contracts. Larry Ingersman is developing the techniques under Bob. CDC is working jointly with IBM (Jack Bertram and Walter Dowd) on this effort. The approach is based on computation pattern analysis against normative profiles of approved application programs. The results of the analysis would be stored in fail-safe devices installed in the CPU from which recordings would be removed to diplomatic safes and couriers. Bob Morris wishes to be the CDC contact for anybody interested in this activity.

I found CDC to be cooperative and willing to work with RISOS.

DIGITAL EQUIPMENT CORPORATION

Ken Olson and Gordon Bell were visited at DEC on 5 January 1972. DEC does not usually get into applications of its computer products to avoid competition with its customers. Security features have not been seriously considered by DEC, since there is no significant customer interest. Metal key locks on computer console panels are the only evidence of security awareness. Ken feels that to a great extent the computing community must rely on mutual trust and ethical practices.

DEC hardware products will become subjects of theft. A technician at DEC stole a PDP-8 a piece at a time and assembled it at home for his own use.

I noted a reasonable level of plant security on my visit. However, the only restrooms for visitors in the main lobby are at the opposite end of what appeared to be the main computer room for software development. I was told to thread my way through a nearly complete set of DEC products in operational use to reach the men's room which I did without an identifying visitor's badge.

HONEYWELL INFORMATION SYSTEMS, INC.

I visited Dr. John Weil at Honeywell Information Systems (HIS) on January 4, 1973; I also talked with HIS personnel engaged in operation of EDP training at Walpole Prison, but this is the subject of another report.

It is my impression that HIS has gone further than any other computer manufacturer in providing controlled access features in standard products with the planned announcement on 17 January 1973 of the HIS 6180 CP. It will incorporate hardware features for access control as developed at MIT Project MAC in the MULTICS system. This is a relatively bold move, requiring all customers to pay for the additional security features whether they want them or not. The market is ambivalent, with the private sector generally uninterested in computer security and the federal sector pushing hard for it in standard products. John thinks the other manufacturers are not taking sufficient responsibility and generally ignoring the need for secure systems or delaying action. He concluded this after attending the recent ONR conference.

John points out that, even if the manufacturer supplies the controlled access capability, it will be useless unless put into an already security-oriented customer environment. He is frustrated in pushing sophisticated security features when so many simpler measures could be taken but are not. He agreed that customers will require secure systems only when they have been frightened into it by major catastrophes or are forced into it through legislation and regulation. The computer industry should be acting as amicus curiae in the coming legislative restrictive actions and resistance of them by the computer users. He encouraged SRI's

work in collecting and documenting factual information of actual computer-related incidents of unauthorized acts causing losses.

John agreed with my theories regarding increasing computer-related crime, decreasing general transactual crimes, and concepts of automation of security to reduce human involvement and the forcing of acts to require collusion. He felt that detection in contrast to prevention is difficult to consider because of the problem of defining the difference between the two. He said that MULTICS has detection as backup to prevention, pointing out that prevention is meaningless unless its performance is detectable. He had not fully considered the concepts of dispersed versus centralized authorization control needs of different environments and referred me to the MIT people who have considered this. He agreed that the problem of proving and certifying the integrity of the hardware and software security features of a system is now the most difficult problem. He suggested the need for special specification and programming languages amenable to proof for security software. I suggested the possible need for a hardware feature for trace-backs of CP control transfers (possibly a register to hold the address of the last jump instruction executed). The HIS MULTICS system does not have the capability but it might prove useful.

HIS has designed a cryptographic product, but there is not sufficient demand for it yet. HIS also has designed a user identification device, but the method used is being kept secret. HIS has rejected voice recognition and hand measurement devices and feels its is superior to others developed so far.

John has formed a full-time computer security development staff in Phoenix. Personnel from this group are planning to visit various security-oriented project sites, including SRI and RISOS.

SINGER BUSINESS MACHINES DIVISION

I visited Dr. Clair Miller, Director of Software for Singer Business Machines in San Leandro, California. Singer has about 60 percent of the point of sale (POS) transaction terminal business. Its largest accounts are Kresge, Woolworth's and Sears. As a division it is now breaking even after several years of losses. Its main products include the System 10 computer system, peripherals, and POS terminals. These terminals are cash registers with special minicomputers with hardwired programs and outputting up to 60 registers of information over a twisted-pair wire at low speed (120 bps) to a poling multiplexer into a computer, a System 10, or IBM computer. One large output register at the terminal is used for computer to terminal messages currently limited to negative credit information to stop a transaction. The terminals can be poled for theoretical inventory status and cash on-hand. Clerk employee numbers and metal keys must be used to LOGON and activate a terminal.

Although it would be expected that security would be of vital importance in such POS products, there has been no customer demand for security features and Singer has little security-oriented product R&D activity. Security research has a low priority, although there is some work on personal identification. I suspect that customers are fitting terminals into cash register environments with little or no change from previous stand-alone facilities. They probably have not yet experienced any different types of POS fraud than in the past and do not appreciate the potential of protection possible in an on-line environment.

John Hunt in San Leandro (357-6800, x2042) heads new product development and would be the appropriate person to contact for further information.

UNIVAC, FEDERAL SYSTEMS DIVISION

I visited the Univac Federal Systems (Eagan) Plant in St. Paul, Minnesota, on December 15. A meeting with about ten people was arranged by Frank Quirk. The group almost entirely represented federally funded product development. Robert Lee heads the Univac Government Computer Security Committee at Arden Hills in St. Paul. However, he was unable to attend the meeting. The meeting consisted mostly of my presentation on threats to computers.

Univac is developing a new computer based on virtual machine concepts for NTDS to be delivered soon to NELC. These concepts have isolation of users and data as a basis thus assuring significant levels of security. At the NBS/ACM Workshop I learned that Clark Weissman at SDC has received a major contract to assist IBM (Joel Birnbaum) at the Watson Research Center in Yorktown Heights on development of virtual machine concepts.

The Univac people stressed the importance of recovery and minimizing false alarms, as well as prevention, detection, and deterrence when considering aspects of computer security.

This meeting was too brief and included too many people to be very effective. In any case they are now aware of RISOS. I recommend meetings with individuals such as Robert Lee mentioned above.

Appendix B

REPORTS ON RESEARCH AND SERVICE ORGANIZATIONS VISITED

Appendix B

REPORTS ON RESEARCH AND SERVICE ORGANIZATIONS VISITED

As partial fulfullment of the SRI contract for Project RISOS at Lawrence Livermore Laboratory, Donn B. Parker visited the research and service organizations listed below.

MIT Project MAC, Cambridge, Massachusetts--Drs. Jerome Saltzer, Michael Schroeder, Robert Scott (5 January 1973).

TRW Systems, Redondo Beach, California--Dr. Eldred Nelson (9 February 1973).

TRW Credit Data, Garden Grove, California--Walter Thyer (9 February 1973).

Tymshare Corp., Cupertino, California--Norman Hardy (22 January 1973).

Rohr Industries, Chula Vista, California (14 March 1973).

Reports of these visits are described by Mr. Parker in the following pages.

MIT PROJECT MAC

On January 5, 1973, I visited Profs. Jerome Saltzer and Mike Schroeder at Project MAC and Mr. Robert Scott at the campus computing facilities at MIT.

Saltzer and Schroeder assume that the MULTICS ring structure has solved the controlled access problem in multiaccess systems except in one respect, its auditability. Their major efforts in solving this problem. will consist of reducing by an order of magnitude in size and complexity the 80,000 instructions and 400 modules of the security functions. They expect this will result in an isolated, simple package understandable by one person and thus made auditable. They believe this is now possible with the MULTICS ring structure hardware features. Other systems such as RSS would require a reduction in complexity and size by two orders of magnitude to do the same thing. Their plans include holding the functional capability of the system constant for now with possible trade-offs to improve cost-effectiveness later. A few nonparallel, dependent functions must be made parallel to simplify those functions. Expanding the types of interrupt processes can now be tolerated, and isolation of the security functions from the general operating system functions will be accomplished. When I mentioned Dan Edward's statement that the only technique he is aware of that could stop him from system penetration is compartmentalization, Saltzer indicated that some aspects of compartmentalization exist in MULTICS but basic design would have to be redone to achieve it fully. It is too late for that now.

I suggested a hardware provision for back tracing of central processor control transfers as I had with John Weil at HIS. (I was told this idea was first reported by Van Horn.) They thought it sounded like a good idea and consistent with their auditability needs and a structured program approach.

A lengthly discussion was held on integrating security control in the central processor versus establishing control in a separate minicomputer-based device. They thought it might be a short range solution to the security problem in present systems. However, for new systems, integration directly into the hardware and software in the system as in MULTICS offers the lowest overhead and efficiency with adequate separation of functions.

The ring structure design provides for distributed authorization control at the user level. In contrast, the IBM RSS design forces a centralized authorization in the person of a security officer and security terminal. In the MIT environment in CTSS, a centralized authorization control proved to be painfully cumbersome to the degree that it was a negative factor in security. Users found it was too much trouble to establish authorized access to their files and programs and handled the problem in informal ways, thus eliminating any system protection. Every organization will have a different configuration of authorization control based on their departmental, project, and work confidentiality makeup. This makes a strictly dispersed authorization control or a strictly centralized control impractical. I was assured that MULTICS will provide a tree structure of authorization control to fit any user organization, although the details of how this is accomplished were not described to me. It is also unknown what the system pays for this flexibility. A study of this subject may be desirable to see what computer systems could provide and what various types of user organizations require.

Bob Scott in the campus facility that is studying and testing RSS reiterated this point. RSS lacks flexibility to shape the security and operating system functions to the ever-changing needs of the organization it is serving. This is doubly important in security matters where modification of the system security software is so dangerous. Bob also pointed out that RSS and IBM OS in general make establishing of files difficult and establishing access authorization doubly difficult, leading to a negative security factor because users won't bother with protective features. Bob emphasized the need for flexibility and ease of use.

TRW SYSTEMS AND TRW CREDIT DATA

A meeting was held at TRW Systems with Dr. Eldred Nelson; Jerry Short, IBM RSS Evaluation Project Manager; and Frank Stepczyk also from that project. At Credit Data, a meeting was held with manager Walter Thyer, Director of the National Data Center; Paul Palermo, manager of Network Analysis; and Leonard Eckhaus, Operations Manager.

TRW Systems is working under contract to IBM on evaluation of the Resource Security System. It is developing security requirements and security software certification methods. Tools to aid in testing such as the TRW Product Assurance Confidence Evaluator (PACE), developed and reported on by J. R. Brown and R. H. Hoffman in the AFIPS FJCC, 1972 Proceedings, are being used. IBM is to supply TRW with an extensive set of software tools used internally by IBM. TRW claims great success in reducing software bugs by using testing tools such as PACE. No structured programming methods were used in the software tested by these tools.

Certification of software methods is being modeled on methods used by the Federal Aviation Agency to certify aircraft. Certification methods development is restricted by limiting approaches to those that are politically acceptable rather than just technically sound. Software development is looked at in four phases: design, implementation, certification, and recertification. Stepczyk indicates that although TRW has identified generic classifications of system penetration methods, this does not help in secure system design.

Dr. Nelson supplied information about a computer-related criminal activity which I have documented elsewhere.

At Credit Data, Thyer, Palermo, and Eckhaus said they could not discuss individual unauthorized acts or threats because of the sensitive nature of their business. However, apparently there have been many problems ranging from bomb threats to theft of credit information. They suggested I talk with Ray Williams, head of TRW Security, and Tony Fortuna, Public Relations for TRW. They showed me a typical threat letter that was highly irrational. The Garden Grove national network facility is located in an obscure, unmarked building behind a branch bank in Garden Grove near Disneyland. Identilogic door control devices are used, but they find the use of card keys too cumbersome and are converting to combination, push-button locks. About 80 girls are employed there to answer telephoned credit inquiries by using CRT terminals running on-line to a large IBM 360 installation in the next room. They do not plan to use RSS but are participating in the RSS study. They rely totally on customer identification numbers to identify authorized sources for information requests. They do extensive non-real-time analysis of activity logs for such detection functions as skip tracing-pattern analysis of sources of credit inquiries regarding an individual as indication of a possible fraud.

Credit Data is not particularly advanced in computer security. However, it is working hard to accomplish better security with limited funding. It is concentrating on security involving their employees such as screening and separation of responsibilities. One suggestion coming out of the discussion was the need to establish the cost of security as a separate line item in the budget to assure proper attention by management. There is much lip service to security but little is done in financial support.

TYMSHARE

I interviewed Norman Hardy, Howard Steadman, Ray Wakeman, and James Fonda at Tymshare's Technical Division in Cupertino, California on January 22, 1973.

Security and reliability are two highly interrelated concerns at Tymshare. When reliability fails, it must be assumed that security does also. Norm Hardy is aware of some of the techniques of system penetration used by Dan Edwards at NSA. He claims these specific techniques would not work in penetrating the Tymshare system. However, the level of effort and skill applied in these examples would most likely result in penetration of the Tymshare system in other ways. Tymshare believes this level of effort could include telephone circuit tapping, and this has created interest in cryptography and protection in message switching activity. A scrambling program is available to customers for protecting files stored in the system. Many Tymshare customers use it. It is also possible for customers to replace Tymshare protective features with their own to change the level of protection. However, protection by holding the algorithms confidential would result in a false sense of security. Confidentiality of protection methods is probably a motivation for doing this anyway.

Tymshare prints the last LOGON date and time for each user at LOGON. This provides a certain amount of protection from theft of services. It was interested in the poaching bit technique used at Stanford. Backup files are dumped on tape once each week and stored remotely. Changed files are dumped on tape daily. Tape handling represents a hazard because it requires real-time operator decisions and actions involving customer and system files. Tymshare is looking at bulk storage devices to replace

most tape usage with one of the benefits being automation of security (minimizing real-time involvement). There is a continuing concern for how much the operations staff should be aware of technical aspects of the system. Norm thought that the operators are bonded.

Jim Fonda had direct knowledge of system penetration activity among other time-sharing companies. In 1969 a considerable amount of accessing was going on between two firms that were supposed to be sharing their technology but were not doing so to the extent agreed on. This resulted in a desire to penetrate each other's systems to check on this. Each knew the other's system making it relatively easy to penetrate. During this period, Tymshare was also penetrated by at least one of these firms. Penetration started with discovery of privileged commands by trial and error. Tymshare error messages helped by informing the user a command was legitimate but that the user did not have high enough privilege status to use it. Penetration required about a month and a half, about 40 hours of terminal time, and a total cost of about $1,000 in terminal service and telephone charges. When Jim came to work for Tymshare in charge of quality control, he assisted in changing the system to prevent the attack methods used.

The ethics of penetrating competitors' computer systems was discussed at length. One position holds that once a user has legitimate access to a system, anything he can find or do is legitimate in the absence of any limiting contractual agreements or official notices to the contrary. The ISD versus UCC case is the only legal precedent being set and covers only cases involving unauthorized LOGONS. There are no accepted industry-wide standards, customs, or practices. It is clear that action by trade associations and individual service companies is much needed. Controlled access must be accompanied by "no trespassing" signs.

ROHR INDUSTRIES

This report is based on a visit to Rohr in Chula Vista (near San Diego) for discussions with Tom Bernard, Director Rohrdata Systems; and Harry Goodell, Vice President of Management Systems and Controls.

Rohr has one of the most advanced on-line computer systems for manufacturing control; 160,000 kinds of parts are manufactured, inventoried, and shipped involving 30,000 shop orders per day through 20 departments requiring 50,000 transactions per day. The system consists of two IBM 360/65 computers, 300 million characters of on-line disk storage and about 200 terminals. Two PD-9 computers on-line to the 65s control a completely automated parts warehouse. Most of the terminals consist of small Touch-Tone pads and voice-answer back speakers hard-wired to multiplexers and served by Wavetek voice-answer-back equipment. Each terminal, the communication line, and its share of a multiplexer costs $22 per month. The system tracks all parts, material, and labor through the entire manufacturing process. It greatly increased productivity, reduced inventories, and reduced staff. For example, the time-keeping staff was reduced from 60 to 15 people.

The system operated with 97 percent accuracy until about one year ago when a labor strike occurred. After the strike ended, accuracy dropped to 70 percent. The system accuracy is totally vulnerable to the accuracy of the input by the workers and dispatchers. Sabotage was suspected but never actually proved. In any case, the solution to the problem required strengthening the security and protection of the accuracy of the system. Several months' effort has brought the system back up to 97 percent accuracy and reduced the possible occurrence of intentional acts or unintentional errors and cheating.

The strike did not involve the automated tracking system. In fact, there is a general feeling of satisfaction and acceptance of the terminal system by the workers. Although they personify the system and the voice they hear, the workers still identify managers as the source of any pressure put on them and watchdogging and inconvenience. They are proud that they "operate a computer" in their work and feel they operate it rather than it operating them. This attitude is partly supported by the AFIPS/Time Survey on the public's attitudes toward computers and refutes the popularity of the "big brother" concern fostered by the public information media. The simple nature of the terminal and voice rather than printed output seems also to be factor in this attitude.

Increased accuracy and security of the system have been achieved in several ways. Editing and checking of the input includes adding check digits to numeric codes and identifiers. Crosschecking of related data is performed. For example, a worker's labor code input is checked with the part numbers of the material he says he is working with to make sure the material is at his work station or in transit. Labor distribution discrepancies are immediately checked by timekeepers who get exception reports at CRT and TTY terminals. Parts and material discrepancies are also handled on-line by a manufacturing control group through the dispatchers. There is additional inherent protection by the system, because the workers never know how much checking is actually going on. They are continually amazed at the ability of management (with the system) to discover errors and discrepancies. This helps keep potential saboteurs and cheaters off balance.

The system is far from foolproof, but continual checking and improving the detection mechanisms goes on. A new systems reliability group of eight systems analysts and programmers has been formed to formalize this process.

Appendix C

OTHER ACTIVITIES

Appendix C

OTHER ACTIVITIES

Conferences attended

1972 Joint Computer Conference, Anaheim, California.

ACM/NBS Workshop on Controlled Accessibility, Rancho Santa Fe, California.

IEE Computer Society COMPCON73, San Francisco, California

International Conference on Computer Communications, Washington, D.C.

IEEE Computer Society Special Interest Workshop on Computer Security, Washington, D.C.

ACM Symposium on Computers and Communications, San Jose, California.

Cases Investigated

Metridata, Louisville, Kentucky (Appendix of the Investigation Manual)

Schneider/PT&T, Los Angeles, California (Report enclosed below)

ISD/UCC, Ward, Palo Alto, Oakland, San Jose, California (Appendix of the Investigation Manual).

EDP training in prisons, Wellesley Hills, Massachusetts (Report enclosed below).

Los Angeles County Welfare fraud, Los Angeles, California.

Donn B. Parker's interview with Jerry Schneider is presented on the following pages, together with a discussion of the implications of EDP training in prisons.

INTERVIEW WITH JERRY NEAL SCHNEIDER

Shig Tokubo of Project RISOS at Lawrence Livermore Laboratory and I met with Jerry Neal Schneider for about two hours at the Airport Marina Hotel in Los Angeles on 16 October 1972. Also present was a friend of Jerry's, Bill Myland, an investor. He and Jerry recorded part of our conversation on television tape. Jerry claimed it was for his own use and for promotional purposes. My interview with Jerry about his acts leading to his criminal conviction and his current business plans was the portion taped. He offered to make a copy of the tape for me.

Jerry is about 25 years old, and electronic engineer graduate from UCLA. He planned his theft of communications equipment in a rational, methodical, purposeful manner. His motives were financial gain, the challenge, and a strong hatred of Pacific Telephone Company because of its lack of concern for customers, the public, and other enterprises. He says he supports capitalistic enterprise otherwise. He claims never to have been in trouble with the law previously. He said he would return a lost wallet to its owner and would not do a dishonest act resulting in a loss to individual people. However, he volunteered that if he saw $10,000 sitting unattended in a store and felt that he could take it without detection, he would and suggested any reasonable person would. He claims the court-appointed psychiatrist told him he was not a criminal type.

His method of gaining the knowledge to perpetrate his acts was quite straightforward. He claims to have posed as a writer doing an article on equipment-ordering systems and was given much information about the PT&T RAMAC ordering system running on an IBM 360 computer in batch mode. He

obtained flow diagrams and instructions for employees from a waste basket. He posed as an employee of other companies and of Pacific Telephone in calls made to the company's RAMAC staff asking them detailed questions about input formats, equipment codes, and delivery site codes. He obtained the account numbers and passwords to access a commercial time-sharing service used by PT&T. The access codes were changed three times, but the new ones were given in Pacific Telephone's news service to customers using the old codes. He claims that he was able to run PT&T programs using its data files to get inventory control and distribution analysis information. It was not clear that he also changed data to account for equipment he stole. He formed the Los Angeles Telephone Company and at least some of his staff knew he was stealing from PT&T. He would telephone into PT&T and order equipment from PT&T staff for delivery at PT&T field sites. The orders were punched on cards and ordering was carried out in batch mode through the RAMAC system. He then went to the sites at about 5 a.m. in a truck that looked like a Pacific Telephone truck and picked up the equipment and bill of lading so that none of the site people knew of missing equipment or of equipment ordered. He insists that nobody within PT&T was in collusion with him. He received all the information he needed from volunteered sources.

He had trouble with his staff because of complaints of low salaries. One employee attempted to blackmail him; when that failed, the employee reported him to the police. He claims the newpaper stories of his acts are almost all fiction.

Jerry has gone into business as a "special agent" in a firm he calls Security Analysts, security consultants in EDP, TWX, P.L., SW. Net. His offices are at 1888 Century Park East, Suite 10, Century City, Los Angeles, California 90067, telephone (213) 277-3266. He claims to offer security consulting services to help firms, especially telephone

companies, to avoid attacks such as he made on Pacific Telephone. He claims PT&T will not do business with him, but he hopes to get a contract with AT&T in New York City to write a report on what he did and how it can be prevented. His method of prevention is to develop EDP security staff who would check all company EDP activities and maintain a responsible security attitude among the EDP staff. He does seem to have thought this out very clearly but has much to learn about EDP security and management principles of security. He claims to have an appointment with the Chief of Security for AT&T in New York, to propose his plan. He is also willing to sell his report to others and says he is planning to write a book. He also claims to be negotiating with Gerald McKnight, an English author who is writing a book on computer security and with whom I also have had some contact.

This encounter with Jerry adds support to my hypothesis that a security system must take into account that the perpetrator will know sufficient methods of access to the system and will know most of the detailed specifications of the computer applications, operating system, hardware, and security methods used. Also it supports the idea that automation of security to eliminate humans from security processes as much as possible and development of pattern and tolerance analysis in the system to detect anomalous actions are among the most important areas of development for increasing security effectiveness.

THE IMPLICATIONS OF EDP TRAINING IN PRISONS

This report is in partial fulfullment of an SRI subcontract with Project RISOS at Lawrence Livermore Laboratory. It is based on previous investigation, a visit with Kurt Van Vlandren and Malcolm Smith of Honeywell in Wellesley Hills, and telephone conversations with William Perrin, a consultant and former director of an EDP education program for the Department of Corrections, State of North Carolina; and Kenneth Thompson, who organized a similar program at Southern Michigan Prison.

This short, preliminary investigation is part of an effort to determine the population of potential perpetrators of unauthorized penetration of computer systems. This population must consist mostly of people with the necessary technical skills, knowledge, and access. My initial conclusion is that EDP courses in prisons demonstrate that professional criminals have an opportunity to acquire the necessary skills, knowledge, and access. However, this source of potential perpetrators is insignificant compared with the many, more successful, professional and white-collar criminals with opportunities for EDP education in high schools, trade schools, inservice training programs, colleges, and universities. Most of the EDP training of convicts occurs in state prisons where inmate students, most of them with underprivileged backgrounds are convicted of violent crimes rather than crimes in which EDP training could be helpful.

William Perrin found 26 states with prison EDP training programs in 1969. Only a small number of prisoners are trained because of heavy screening and aptitude restrictions. The program at Walpole prison supported by Honeywell has resulted in 63 paroled graduates in five

and one-half years with about one-third known to have entered the EDP field. While general rates of recidivism among state prisons are 60 to 70 percent, recidivism among the EDP program graduates is less than 6 percent in Massachusetts and North Carolina. Graduates tend to get jobs in government organizations where they had obtained in-prison work previous to parole. Prisoners form companies while in prison to perform work on outside contracts. Courses are often taught by more advanced inmate students. Courses cover programming languages, business mathematics and administration, hardware maintenance, systems analysis, and occasionally advanced systems programming. Of 20 recent graduates from Walpole, Honeywell employs three, DEC has one, the State Department of Education has one, and the City of Newton Education Staff has one. One graduate, over 50 years old, spent most of his life in prison; he never held a job for more than a day during years of freedom and was almost a living vegetable in prison. Programming sparked life into him, and he is now a successful systems programmer with a computer manufacturer.

Ex-convicts are normally hired in EDP with full knowledge and cooperation of the employers. An employer with strong management, adequate security, including separation of sensitive responsibilities, should have no qualms about hiring an ex-con. His background will always be well known. He lives under strict personal performance rules while on parole, and a good-paying job which he has probably never had before creates an environment in which he is probably highly motivated to make good. He also knows that if any unauthorized actions occur in his working facilities, he will be the first to be blamed. He may be torn by two conflicting forces if confronted by such a situation. Cooperation in apprehending the perpetrator keeps his reputation clean and improves his chances, but the unwritten law among convicts and ex-convicts forbidding "ratting" may be more influential. Ex-convicts are prime targets for extortion and influence by former criminal associates

possibly forcing them to perpetrate unauthorized acts. This must be particularly guarded against. Nonetheless, the fact that they are "known quantities" makes them attractive potential employees when hired in small numbers for rehabilitation purposes.

Among 100 cases of computer-related acts none has yet been discovered to have been committed by ex-convicts.

Appendix D

QUESTIONNAIRE FOR DOCUMENTING COMPUTER-RELATED INCIDENTS OF INTENTIONALLY CAUSED LOSSES, INJURIES AND DAMAGE

Part 1. Case ID _____ Coding

Earliest Date of Act _____

Date of This Report _____

Revised Date _____

COMPUTER-RELATED INCIDENT QUESTIONNAIRE

PART 1. CASE IDENTIFICATION

1.1 Case name _____

1.2 Brief case description _____

1.3 Key words extracted from 1.2

1.4 Names of computer systems involved (operating organization and generic type)

1.5 Case locations. Cities and local sites of acts, targets, perpetrators

1.6 Participants. Victims, suspected perpetrators, prosecutors, witnesses

	Role played	Name	Title, Address, Telephone
A			
B			
C			
D			
E			

(Form revised 12/72 D. B. Parker)

Case ID _____

1.7 Type of investigation and sources. Identify all applicable items by inserting names of sources and dates

		Dates
On-site investigation		
Telephone calls		
Letter correspondence		
Face-to-face interview		
Directly quoted		
Document extraction		

1.8 Authors of this questionnaire _____

_____

Revision by _____

1.9 Case investigators _____

_____

1.10 Case documents	Location

Case ID _____

COMPUTER-RELATED INCIDENT QUESTIONNAIRE

PART 2. ENVIRONMENTS OF THE ACT

2.1 Computer systems involved in the case. (Use one form for each system).

2.1.1 System identification _____

Operating Organization	Facility Locations	CPU Vendor, Model, Storage	Mode of Operation	Purposes

2.1.2 Peripherals pertinent to the case _____

2.1.3 Operating system, options, modifications, add-ons _____

2.1.4 Software packages pertinent to the case _____

2.1.5 Terminals pertinent to the case

No.	Make	Model	Location	Ownership	Purposes

2.1.6 Communication system (multiplexers, concentrators, circuit types, and their locations) _____

2.1.7 Type of computer system application. (Circle letters. More than one type may apply at different times.) a. Transaction system. b. More than one transaction subsystem. c. Transaction subsystems and programmer access. d. Programmer access at application language level. e. Programmer access at machine language level. f. Other _____

2.1.8 Type of access authorization control. (Circle letters. More than one type may apply at different times.) a. None. b. Centralized authority granting. c. More than one can grant authority. d. Individual users can authorize others. e. Other _____

2.1.9 Security levels present. (Circle letters. More than one type may apply at different times.) a. System and contents open to all users. b. Part of system and/or contents requires authorized access and part is open to general access. c. More than one level of authorized access in addition to general access. d. More than one level of authorized access and no part is open to general access. e. All access must be authorized. f. Other _____

2.1.10 Degrees of confidentiality of the contents of the system. (Circle all appropriate letters.) a. U.S. Government classified (national security). b. Personal or organizational safety (compromise would cause personal unrecoverable injury or death or organizational failure). c. Personal or organizational integrity (unrecoverable injury, damage or loss). d. Personal or organizational recoverability (recoverable injury, damage or loss). e. Personal or organizational convenience (irritational injury, damage or loss). f. Public domain (no confidentiality). g. Other _____

2.1.11 Number of employees dedicated exclusively to computer system protection (Supply numbers). EDP auditors a._____ Guards b. _____ Data validation/ control clerks c._____ Other d._____

2.1.12 Staff contacts (operations, systems, applications, hardware maintenance, EDP audit, security) _____

_____

_____

_____

Case ID_____

2.2 "Quick-check" system characteristics (Use one set for each system)

System identification _____

(Circle appropriate numbers)

1. Local batch
2. Remote batch
3. Time-sharing
4. Multiaccess
5. Time-slicing
6. Multiprogrammed
7. Multiprocessors
8. Single mode of operation
9. Multimode, simultaneous
10. Multimode, sequential
11. Network-connected
12. Hierarchically-connected, head end
13. Hierarchically-connected, subsystem
14. Data communications used
15. Multiplexers on-site
16. Remote Multiplexers
17. Concentrators on-site
18. Remote concentrators
19. High speed circuits ($\geq$9600 bps)
20. Low speed circuits ($<$9600 bps)
21. Dial-up circuits
22. Private circuits
23. Leased circuits
24. Microwave
25. Half duplex
26. Full duplex
27. Synchronous
28. Asynchronous
29. Conversational terminals
30. Batch or job terminals
31. Transaction terminals
32. Graphics terminals
33. Telemetry terminals
34. Real-time, process control terminals
35. Conversational terminal response
36. Performance monitoring devices
37. Tape drives
38. Disk drives, permanent
39. Disk drives, removable
40. Magnetic drums
41. Add-on core storage
42. Paper tape
43. Mass storage, optical
44. Multivendor central configuration
45. Paged storage, hardware
46. Paged storage, software
47. Virtual storage, hardware
48. Virtual storage, software
49. Relocation feature
50. Hardware storage protection
51. Privileged instructions
52. Continuous operation
53. First shift only
54. Two shifts
55. Three shifts
56. Weekend, holiday operation
57. Dedicated to one (few) applications
58. Business applications
59. Engineering applications
60. Research applications
61. Integrated file applications
62. Process control applications
63. Transaction applications
64. U.S. Government classified processing

65. All access local to system
66. Multiple customers (corporations)
67. Service bureau operation
68. Operation shared with other companies
69. Operation by a service company
70. Maintenance by CPU vendor
71. Maintenance by independent service
72. Multivendor maintenance
73. In-house maintenance
74. CPU-vendor supplied operating system
75. Independent vendor operating system
76. In-house operating system
77. Modified vendor operating system
78. More than one operating system used
79. On-line user-program library
80. On-line application files
81. Files encrypted
82. Data encryption optional
83. Data communication hardware encryption
84. Data communication software encryption
85. Terminal identification by hardware

Terminal LOGON by

86. User ID
87. Password
88. Single-use password
89. Account code
90. Site code
91. Dialog with user
92. Time limit
93. Error limit
94. Portable key or card

95. Security features integrated in OS
96. Security features added on
97. Security features in isolated modules
98. Centralized access authorization
99. Decentralized access authorization
100. OS isolated from users
101. Users' jobs isolated from each other
102. File access restricted by authorization
103. First write before read data protection
104. Storage erasure after use
105. I/O buffers, registers cleared after use
106. Access authorization data in files
107. Access authorization in file index tables
108. User access to assembly-level language
109. File activity tracing or auditing
110. Security monitoring of system use
111. Real-time human monitoring of security
112. Console dedicated to security functions

Remote back-up storage of

113. Operating system
114. Application programs
115. Data files

116. Removable storage devices stored local to drives
117. Positive door access control to facilities
118. Programmers' and operators' work areas separated

Case ID _____

COMPUTER-RELATED INCIDENT QUESTIONNAIRE

PART 3. DESCRIPTION OF THE ACTS AND DETECTION

3.1 Type of act. (Circle applicable letters)

a. Unauthorized use of the services of computer systems.

b. Unauthorized sale of the services of computer systems.

c. Unauthorized taking of information, computer programs or property or copies thereof.

d. Direct financial gain by taking negotiable instruments or transferring monetary credit.

e. Vandalism.

f. Other _____

_____

3.2 Access and methods used to perpetrate the acts

3.2.1 Is physical access to the sites of the acts applicable and pertinent to this case? yes no

3.2.2 Physical access: times and days _____

(Circle appropriate letters and prefix capital letters to identify suspects)

___a. Covert access. ___b. Overt access. ___c. Authorized. ___d. Unauthorized. ___e. Assisted by others. ___f. Tools or devices used to gain entry. ___g. Observed by others. ___h. Impersonation used. ___i. Access reported to responsible persons. When? _____

_____

___j. Diversion tactics used. Describe _____

_____

3.2.3 Were the sites of the acts protected by: (Circle appropriate letters)

a. Locked doors. b. Guards. c. Electronic/optical devices. d. Not protected. Describe _____

_____

3.2.4 Methods and devices used: (Circle appropriate numbers and prefix capital letters to identify suspects) ___1. On-line. ___2. Off-line. ___3. Conversational terminal. ___4. Transaction terminal. ___5. Job entry terminal. ___6. Computer console. ___7. Security console. ___8. Supervisory terminal. ___9. Maintenance console. ___10. Direct manual action. ___11. By issuing instructions to other people.

___12. Off-line program manipulation. ___13. Off-line job control manipulation. ___14. Terminal commands. ___15. Immediate results. ___16. Delayed results. ___17. On-line program manipulation. ___18. By impersonation. ___19. Program impersonation. ___20. Operating system penetration. ___21. Violation of program boundaries. ___22. Violation of data storage boundaries. ___23. Violation of parameter value ranges. ___24. Simulation of an authorized function. ___25. Covert. ___26. Overt. ___27. New program. ___28. Existing program. ___29. Utility program. ___30. Unauthorized use of identification codes. ___31. Covert use of communication circuits. ___32. Disguised as an accident. ___33. Accident or error used. ___34. Overloading of a system activity. ___35. Overloading of a manual activity. ___36. Diversion used. ___37. Input data manipulation. ___38. Output modification. ___39. Subversion of protective features. ___40. Procedural modification. ___41. System breakdown (crash) necessary for perpetration of the act. ___42. Standard operating procedures used. ___43. Non-standard operating procedures used. ___44. Information, programs or property taken from a person by force. ___45. Information, programs or property taken from a person by deception. ___46. Other _____

3.2.5 Narrative description of methods and devices used. _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

3.2.6 Key words used above: _____ _____ _____

_____ _____ _____ _____

_____ _____ _____ _____

Case ID _____

3.3 Goals, Targets and Results

	a. Unauthorized removal	b. Unauthorized usage	c. Used in unintended ways	d. Unauthorized removal of a copy	e. Unauthorized modification	f. Total destruction	g. Reparable damage	h. Not achieved	i. Achieved partially	j. Achieved totally	k. Results unintended by suspects
3.3.1 Hardware											
1. CPU											
2. Storage											
3. Channels											
4. Controllers											
5. Peripherals											
6. Cables											
7. Terminals											
8. Communications devices											
9. Communication circuits											
10. Parts inventory											
11. Monitoring devices											
12. Security devices											
13. Other _____											
_____											
3.3.2 Media											
15. Disk packs											
16. Magnetic tape (mini or cassette)											
17. Paper tape											
18. Punch cards											
19. Film											
20. Printer paper, carbon paper											
21. Printer ribbons											
22. Other _____											

Case ID _____

3.3.3 Software

22. Application programs
23. System of application programs
24. Library of application programs
25. Job control instructions
26. Operating system
27. Supervisor
28. Job scheduler
29. Queueing control
30. Interrupt processor
31. Job swapper
32. Resource allocation
33. Storage manager
34. I/O processors
35. Operator control
36. Accounting
37. Recovery
38. System initialization
39. System bootstrap
40. Library manager
41. Job control translator
42. Terminal manager
43. Activity monitor
44. Performance monitor
45. Access controller
46. Authorization controller

	a. Unauthorized removal	b. Unauthorized usage	c. Used in unintended ways	d. Unauthorized removal of a copy	e. Unauthorized modification	f. Total destruction	g. Reparable damage	h. Not achieved	i. Achieved partially	j. Achieved totally	k. Results unintended by suspects

Case ID _____

	a. Unauthorized removal	b. Unauthorized usage	c. Used in unintended ways	d. Unauthorized removal of a copy	e. Unauthorized modification	f. Total destruction	g. Reparable damage	h. Not achieved	i. Achieved partially	j. Achieved totally	k. Results unintended by suspects
47. I/O drivers											
48. Compilers, assemblers, translators											
49. Utility programs											
50. Other _____											
_____											
3.3.4 Data											
51. Stored on-line application files											
52. Stored off-line application files											
53. Machine-readable input data											
54. Machine-readable output data											
55. Input data for conversion											
56. Output reports											
57. Operations records											
58. Active operating system tables, files											
59. Security authorization tables											
60. User identification tables											
61. System monitoring files											
62. Buffer files											
63. Queueing files											
64. Other _____											
_____											
3.3.5 Documents											
65. System software manuals											
66. System user manuals											

	a. Unauthorized removal	b. Unauthorized usage	c. Used in unintended ways	d. Unauthorized removal of a copy	e. Unauthorized modification	f. Total destruction	g. Reparable damage	h. Not achieved	i. Achieved partially	j. Achieved totally	k. Results unintended by suspects
67. System software specifications											
68. System design documents											
69. System usage aids											
70. System newsletters											
71. Maintenance documents											
72. Hardware manuals											
73. Hardware drawings											
74. Operator instructions											
75. System status reports											
76. Data control instructions											
77. Audit documents											
78. Security documents											
79. Data preparation instructions											
80. Application manuals											
81. Application specifications											
82. Organization procedures, charts											
83. Personnel lists											
84. Published reports, papers											
85. Unpublished reports, papers											
86. Other _____											
3.3.6 Facilities											
86. Doors											
87. Windows											
88. Walls											
89. Floors											

Case ID _____

	a. Unauthorized removal	b. Unauthorized usage	c. Used in unintended ways	d. Unauthorized removal of a copy	e. Unauthorized modification	f. Total destruction	g. Reparable damage	h. Not achieved	i. Achieved partially	j. Achieved totally	k. Results unintended by suspects
90. Ceilings											
91. Locks											
92. Safety equipment											
93. Power supply											
94. Oral communication equipment											
95. Air conditioning equipment											
96. Lights											
97. Security alarms											
98. TV equipment											
99. Photographic equipment											
100. Furniture											
101. Furnishings											
102. Data keying devices											
103. Off-line processors											
104. Other _____											
_____											

3.4 Actions taken by suspects to avoid detection (Insert capital letters to identify participants).

	Restore a.	Change b.	Destroy c.	Remove d.	Contributed to Detection e.
1. System logs					
2. Security log					
3. Program changes					
4. Data changes					
5. Label or name changes					
6. Programs					
7. Data					
8. Buffer contents					
9. Storage contents					
10. Fingerprints, pictures					
11. Waste materials					
12. Moved equipment					
13. Moved media					
14. Moved materials					
15. Telephone circuit usage log					
16. Other _____					
17. _____					

3.4.1 Describe _____

_____

_____

_____

3.4.2 Detection. (Circle appropriate letters) a. Before acts could occur.

b. During acts. c. After acts, time period _____.

d. Accidental discovery. e. By established detection methods.

f. Suspects identified. g. Suspects caught.

3.4.3 Participants in detection and suspect identification. (Use capital letters to identify participants.)

1. Computer operations staff		
2. Security staff		
3. Audit staff		
4. Systems programming staff		
5. Hardware maintenance staff		
6. Applications staff		
7. Janitorial staff		
8. Vendor's staff		
9. System users		
10. Customer support staff		
11. Other _____		

3.4.4 Describe detection _____

_____

_____

_____

_____

_____

3.5 Suspects' positions relative to the acts and systems involved. (Circle appropriate numbers and prefix capital letters to identify suspects.)

___1. Computer system management. ___2. Company management. ___3. Application programmer/analyst. ___4. System designer. ___5. System programmer/analyst. ___6. Program maintenance. ___7. Auditor. ___8. Data clerk. ___9. Security guard. ___10. Building maintenance worker. ___11. Hardware maintenance engineer. ___12. Data conversion operator. ___13. Computer/peripheral operator. ___14. Courier or messenger. ___15. Outside consultant. ___16. Company employee (not in computer system staff). ___17. Vendor's employee, on-site. ___18. Vendor's employee, off-site. ___19. Internal customer of system. ___20. External customer of system. ___21. Business competitor's employee. ___22. Business associate employee. ___23. A person involuntarily served or affected by the computer system. ___24. A person voluntarily served or affected by the computer system. ___25. Social or political dissident. ___26. Other ____ _____. ___27. Other _____

3.5.1 Knowledge and experience of the suspects. (Identify each suspect by a capital letter. Multiple entries for a single box are acceptable.)

	a. Knowledge	b. Experience	c. Not authorized	d. Authorized	e. Of systems involved in these acts	f. Necessary to accomplish the acts	g. Faulty knowledge or error resulting in failure	h. Faulty knowledge or error resulting in detection
1. Access to facilities								
2. Operation of terminals								
3. Operation of peripherals								
4. Operation of communications								
5. Operation of computer								
6. Job submission								
7. Access identification								
8. Data submission								
9. Data preparation								
10. Data conversion								
11. Data control								
12. Application program use								
13. Application program modification								
14. Application programming								
15. Systems programming								
16. Operating system modification								
17. Computer modification								
18. Peripherals modification								

Case ID _____

	a. Knowledge	b. Experience	c. Not authorized	d. Authorized	e. Of systems involved in these acts	f. Necessary to accomplish the acts	g. Faulty knowledge or error resulting in failure	h. Faulty knowledge or error resulting in detection
19. Terminals modification								
20. Communication modification								
21. Wiretapping								
22. Radiation pickup								
23. System security modification								
24. System auditing								
25. System testing								
26. Acquainted with staff								
27. Acquainted with users/customers								
28. Organization procedures								
29. Staff working schedules								
30. System schedules								
31. Independent training course								
32. Internal training course								
33. Other _____								

3.6 Estimate of value of losses, injuries and damages: $_____

3.7 Changes made in the computer system as a result of these acts. Security increased? yes no Describe _____

_____

_____

_____

_____

_____

3.8 Most important implications of this case _____

3.9 Additional information _____

COMPUTER-RELATED INCIDENT QUESTIONNAIRE

PART 4. SUSPECT INVESTIGATION (One form for each Suspect)

4.1 Interviews

Date	Interviewer	Interviewee	Location

4.2 Background

4.2.1 Name _____ Age _____ Sex _____

4.2.2 Home address _____

_____ Telephone _____

4.2.3 Work address _____

_____ Telephone _____

4.2.4 Education (Circle) High school 1 2 3 4 years. Location _____

College 1 2 3 4 years. Locations _____

Degree	Subject	Institution	Year

Professional society membership _____

4.2.5 (Circle appropriate letters) a. Married b. Separated c. Divorced d. Widowed e. Single Children: Age ___ Age ___ Age ___ Age ___

4.2.6 Present employer _____ Years _____

Occupation or title _____

Brief job description _____

_____

4.2.7 Other business interests _____

_____

4.2.8 Salary (Circle a letter) a. less than $6000 b. 6000-7999 c. 8000-9999 d. 10,000-13,999 e. 14,000-17,999 f. 18,000-23,999 g. 24,000-29,999 h. 30,000-39,999 h. 40,000-49,999 i. More than 50,000

4.2.9 Recent employment (Most recent first)

Employer	Position	From	To

4.2.10 Criminal history. Number of arrests _____ Number of convictions _____

Arrest Charges	Date	Disposition

4.3 Suspect's involvement in the incident.

_____

_____

_____

_____

_____

_____

4.4 Before the acts

4.4.1 Purpose of the acts (Circle appropriate letters). a. Direct financial gain by acquiring a negotiable instrument or transfer of credit. b. Indirect financial gain by converting results of the acts to financial gain. c. Personal advancement. d. Revenge. e. To support ideals. f. To right a wrong. g. A challenge. h. Curiosity. i. Self-amusement. j. Amusement of others. k. To help somebody else. l. Other _____

_____

4.4.2 Source of the idea for perpetrating the acts. (Circle appropriate letters.) a. Accident or error demonstrated the possibilities. b. Learned of similar acts. c. Had performed similar acts. d. Associates or friends performed similar acts. e. Associates or friends talked about similar acts. f. Exposure of the target represented a temptation. g. Apparent ease of the acts represented a temptation. h. Other _____

_____

4.4.3 Attitude of the suspect towards potential individual, personal victims, if any. (Circle appropriate letters) a. Sorry. b. Sympathetic. c. Hostile. d. Superior to them. e. Inferior to them. f. Indifferent. g. Other

_____

4.4.5 Other similar acts suspect was aware of.

Act	Source

4.5.2 Actions (Circle appropriate letters) a. Compulsive. b. Frightened. c. Confident. d. Methodical. e. Disorganized. f. Followed plans. g. Deviated from plans. h. Encountered unexpected situations. i. Aware of witnesses. j. Careful to remove evidence. k. Not concerned with evidence. l. In collusion with others. m. No collusion. n. Required cooperation of innocent people. o. No cooperation of others required. p. Actions were against a system. q. Actions were against people. r. Posed or disguised as somebody else. s. Acted under his own identity. t. Fearful of detection. u. Not fearful of detection. v. Successful. w. Partially successful. x. Not successful.

4.5.3 Collusion in the acts (Place an asterisk before name of the leader if not the suspect)

Name	Relationship to Suspect	Nature of Involvement

4.5.4 Witnesses

Name	Relationship to Suspect	Nature of Involvement

4.5.5 Suspect disguised or posed as _____

_____

4.5.6 Mistakes and deviation from plans _____

_____

_____

_____

4.5.7 Reasons for success or failure _____

_____

_____

4.6 After the acts

4.6.1 (Circle appropriate letters) a. Eager to discuss his actions. b. Willing to discuss his actions. c. Unwilling to supply information. d. Left the scene of his actions normally. e. Left the scene in haste or abnormally.

4.4.6 Planning. (Circle appropriate letters) a. Acts were not planned. b. Acts were partially planned. c. Acts were completely planned. d. Planning was a full time effort. e. Planning was a part time effort. f. Cost of the acts was estimated. g. Risk was evaluated. h. Sanctions if caught were known. i. Avoidance of discovery was planned. j. Discovery was expected after the acts were perpetrated. k. If caught, exposure to family, friends or associates was feared. l. If caught, public exposure was feared. m. Certain of carrying out plans. n. Uncertain of carrying out plans. o. Would be successful even though caught or exposed. p. Would not be successful if caught or exposed. q. Confident of success. r. Not confident of success. s. Was not aware of criminal nature of the acts. t. Was not aware of unethical, unfair or immoral nature of the acts. u. A change in protection of the system could have aborted plans. v. New knowledge required. w. New knowledge not required. x. New skills required. y. New skills not required. z. Planning included other participants. * Act planned from a position of trust.

4.4.7 New skills acquired _____

_____

_____

4.4.8 New knowledge acquired _____

_____

_____

4.4.9 Collusion (Place an asterisk before name of the planning leader if not the suspect)

Name	Relationship to Suspect	Nature of Involvement
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

4.4.10 Date act was first conceived _____

By whom _____

4.4.11 Planning period. From _____ to _____

4.5 During the acts

4.5.1 Period of time to conduct the acts (date, time). From _____

_____ to _____

f. Sees himself as a hero. g. Is remorseful. h. Is self-righteous. i. Is indifferent. j. Is elated. k. Shows animosity toward victims. l. Shows animosity toward other involved parties. m. Believes his actions were appropriate for the circumstances. n. Feels he was wrong in his actions. o. Would repeat the actions under similar circumstances. p. Would never repeat his actions. q. Willing to make restitution. r. Not willing to make restitution. s. Feels he made a net gain towards his objectives. t. Suffered a net loss towards his objectives.

4.6.2 What did the suspect fear most (Rank by numbers or leave blank if not applicable)

a. ___ Discovery of the act
b. ___ Exposure of him as the perpetrator
c. ___ Harm to others
d. ___ Punishment
e. ___ Publicity
f. ___ Other _____
g. ___ Other _____

4.6.3 Feelings towards other involved parties

Name	Feelings

4.6.4 What circumstances would have stopped the suspect's actions? _____

_____

_____

_____

4.6.5 Alternative actions suspect could have taken:

Action	Reason for Rejection

Appendix E

PROJECT PROGRESS REPORT
December 20, 1972

20 December 1972

Progress Report 1
Covering the Period 19 September through 31 December 1972
Stanford Research Institute Project 2194

TECHNICAL SERVICES

by
Donn B. Parker

Contract P/A No. 91 Under AT(04-3)-115

Prepared for

U.S. Atomic Energy Commission
University of California
Lawrence Livermore Laboratory
P.O. Box 808
Livermore, California 94550
Attn: Ivan Morvay L379

Copy No. ____

I PURPOSE

The purpose of the work performed is to provide the results of an investigation of computer installations and computer manufacturers to identify those installations in which information has been compromised by unauthorized persons.

II TECHNICAL PROGRESS

The first draft of a questionnaire to be used by an investigator of incidents of intentional, unauthorized access to multiaccess computer systems was completed on October 2, 1972. It was based on a questionnaire developed previous to this project and one designed by Judy Ford of the RISOS Project. The questionnaire was reviewed for technical accuracy, completeness,and applicability by Dr. Peter Neumann and Mr. Carrol Kerns, SRI Information Sciences Division, and by Dr. Brian Parker, a forensic scientist. Critiques were received in the form of annotated copies of the questionnaire. The RISOS project personnel reviewed the document in detail.

The first draft proved to be too long, too wide in scope covering items not of particular interest to RISOS,and there was not enough depth of items concerning technical aspects of the operating systems and hardware constituting the objects of attack.

The second draft, satisfying the critiques of the first draft, was sent to RISOS on November 29, 1972. Mr. Steven Oura, a sociologist at SRI, reviewed the suspect section of the questionnaire. The final draft will include his suggestions. Otherwise, only minor problems were identified by the RISOS staff.

The draft questionnaire was used to document the ISD vs UCC Program Theft case from documents collected and investigations made before this project started. This test revealed a number of shortcomings in the practical areas of sufficient space for answers, ambiguous and unclear wording of questions,and depth of details.

The second draft questionnaire was also used in a new investigation of the Cincinnati/Louisville Time-Sharing Use Fraud case that occurred in 1970. This test also resulted in new insights into the questionnaire content and format.

The Cincinnati/Louisville case investigation resulted in refining some techniques in field investigation that will be used in developing a manual on this subject. This was an appropriate case because it involved travel to an unfamiliar site, unfamiliar computer system environment, and a relatively sophisticated method of unauthorized access and attack on the operating system of a multiaccess service.

I have also assisted Doug Webb of RISOS in his investigation of EDP audit techniques. I supplied him with documents, information from my field research in EDP audit,and sources of information.

III TRIPS, MEETINGS AND PRESENTATIONS

Meetings were held with the RISOS Project staff on October 3, November 7, and December 7 in 1972. The first was a presentation describing my previous research activities and results. The other two meetings were held to review the questionnaire drafts and exchange intelligence information about activities in computer security research. The RISOS staff gave me assistance concerning computer penetration incidents and contacts among computer manufacturers.

I attended the NBS/ACM Workshop on Controlled Access on December 11-13 in Rancho Santa Fe. I chaired an ACM SIGCOSIM session at the FJCC in Anaheim on December 4 at which Bob Abbott served as a panelist. Two meetings were arranged with Jerry Schneider, convicted of perpetrating a computer-related theft. One meeting was attended by Shig Tokubo, the other by Bob Abbott. A report on the first meeting with Schneider was prepared and submitted to Bob Abbott.

Unauthorized use of computing services was investigated at the Stanford University Computation Center on November 28 and at Metridata Time-Sharing Service in Louisville, Kentucky, on December 14. A trip was made from Louisville to Minneapolis where a day was spent talking with people concerned with security at Control Data and Univac. Reports of these meetings and investigation results are being written.

APPENDIX F

THIRTY-EIGHT CASE HISTORIES

APPENDIX F (continued)

Case Date/Code	Source	Verified	Type	Principals	Disposition	Description
10/11/72 6923	10/11/72	No	Theft	MIT, victim; MIT campus Patrol	Conviction	A student stole a PDP8 computer from MIT, Boston.
1/5/72	Digital Equipment 1/5/72 (see Boston trip notes)	Yes	Theft	Digital Equipment Corp., Victim; employee, thief.	Private sanctions	An employee removed a PDP8 computer from the manufacturing plant a piece at a time and assembled it at home. He was fired.
8/14/72 7236	Keith Marcellius, ISD, Oakland	No	Fraud	Oakland, victim; head of Data Processing Division		Employee fraud.
1970 7045	Robert Wright Metridata, Louisville, Ky. 12/14/72 Charles Mc Guiness, GET.S., Bethesda, Md.	Yes	Theft of services	Fla., victim; two engineers in Detroit, perpetrators.	No action except termination of services	Two engineers accidently used a password one digit different than theirs. It belonged to the president of Compu-time and allowed access to privileged customer and accounting data. Thus it allowed the engineers to use unlimited amounts of computer time and obtain customer information and proprietary program listing. Discovery was made by computer operators who noticed use of the password at unusual times.
1972 7244	Protected source	Yes	Theft of services	Protected victim; perpetrator	Restitution made.	A high school student found a privileged password of the services analyst on a listing in a waste basket. He also obtained detailed specifications of the system. He used large amounts of computer time, played computer games, and obtained other customers' data. He

APPENDIX F (continued)

Case Data/Code	Source	Verified	Type	Principals	Disposition	Description
						was discovered when a computer operator noticed scratch tapes being read before being written.
? 7237	Les Grey, SRI 12/26/72	Yes	Embezzlement	Painting contractor, victim; controller, perpetrator	Controller was fired	Controller embezzled by setting up dummy vendors in accounts payable. Actions were discovered when Grey, as a Burroughs analyst, converted to a new system.
1972 7215	Mervin Miller World Bank, Dr. University Computer Center	Yes	Vandalism	University, victim; student, perpetrator		A student gained priviliged access to the time-sharing system and caused frequent crashes. Malicious mischief.
1967 6741	Datamation 12/67, p. 78	No	Unathorized use of equipment	Chicago Board of Education, victim; five employees, including director of the bureau James A. Quinn, suspects.	Investigation	Five employees operated their own data processing firm using an input scanner of their employer's. All resigned.
1972 7341	Computer World	No	Sedition and hostility to the state	Zagreb, Yugoslavia University data processing center, victim; five students suspects.	Arrested	Five students replaced business output data with antigovernment slogans.
1973 7341	Computer World 1/24/73	No	Fraud	100 Michigan insurance policy holders, victims; agent for United Presidential Life Ins. Co., suspect. Robert Rowe, David Feintuch, Mich. Commerce Dept., Ins. Bureau, prosecutors	Investigation	Agent used computer analysis of life insurance to confuse policyholders saying the computer recommended his policy over theirs.

APPENDIX F (continued)

Case Data/Code	Source	Verified	Type	Principals	Disposition	Description
1972 7238	London Times 5/31/72 B. J. Benzimwa 1/26/73	No	Embezzlement £3,000	Westminster Bank, victim. Several staff, perpetrators.	Convicted	Staff defaced MICR characters on their checks after crediting to payee's accounts. When checks were rejected in reader, they destroyed them, stopping debiting to their own accounts.
1972 72210	Data Banks in a Free Society, Westin Baker, Quadrangle. p. 139	No	Fraud	TRW Credit Data, victim; former employee, perpetrator	Not found	A former employee obtained credit reports by using the identification number of a legitimate subscriber. The number was changed.
1972 72211	Data Banks in a Free Society, Westin Baker, Quadrangle . p. 139	No	Fraud	TRW Credit Data, victim; employee, perpetrator	Fired	An employee tried to change information about himself. A keypunch operator discovered him when she thought it unusual that an employee would submit forms changing his own record.
1972 7239	California State Welfare Dept. 11/27/72	No	Fraud	L.A. County Social Welfare, victim		Welfare grants are paid from vouchers and punch cards. An employee put extra cards in computer to produce unauthorized grants. No suspects identified.
1973 7311	Bob Hargraves, Dartmouth 3/5/73	Yes	Vandalism	Dartmouth Kiewit Computer Center, victim; student at Bates College, perpetrator	No action taken	A student with low-level privilege used a Trojan Horse technique within a file maintenance program he wrote. The program checked privilege level when an operator ran it at privileged level, it took over the executive and invoked another resident privileged program that removed all evidence of penetration. Systems programmers discovered the extra, privileged program in a core dump. Logical AND of privilege and ID of each program set for maximum privilege solved the problem.

APPENDIX F (continued)

Case Date/Code	Source	Verified	Type	Principals	Disposition	Description
1973 7312	Charles Rosen, SRI, 2/6/73	Yes	Vandalism	Ca. victim; computer facilities		Employees returning from a strike sabotaged the on-line parts inventory and ordering system.
1972 72212	2/9/73	Yes	Theft of programs	Software Leasing Corp., James Craigle, suspect		A blind man and James Craigie convineed programmers to take software from their employers and sell it to Software Leasing which then markets the software.
1972 72213		Yes	Theft of programs	McDonnell Douglas victim	One employee fired; one died of a heart attack	Two employees took program listings describing secret processes to be patented. Both employees were seheduled for layoff.
1972 72214	2/9/73	Yes	Theft of dossiers for sale	London, victim		An employee was selling dossiers for £5 on the London black market. He obtained them from an on-line B6700 data bank. He was caught by a program change that trapped on a preassigned name in the file.
1971 71310	Reiner von sur Muhlen, Wirtsehaft und Politik 10/10/71, insurer	No	Payroll theft 280,000DM	Industrial Co. in Solingen, Ger., victim	Employec was foreed to make restitution	An employee changed punch eard input to change employee salaries soon after eonversion to the computer. Management noticed the high salaries and a surprise audit resulted in apprehension
1971 71311	Reiner von sur Muhlen, Wirtschaft und Politik 10/10/71, eomputer manufacturer	No	Pension theft	West German ehemieal firm, vietim		An employee in EDP altered deeeased employee's data to have the deeeased's pension paid into his own bank aecount.

APPENDIX F (continued)

Case Data/Code	Source	Verified	Type	Principals	Disposition	Description
1971 71312	Reiner von sur Muhlen, Wirtschaft und Politik 10/10/71 computer manufacturer	No	Pension theft	Canadian Ins. Co., victim	Apprehended	An employee changed several deceased insured persons' account numbers to his own to collect their pensions. He was caught when a staple in a punch card forced manual handling which revealed several cards with the same number.
1971 71313	Reiner von sur Muhlen, Wirtschaft und Politik, 10/10/71, computer manufacturer	No	Pension Theft		Apprehended	An employee was caught leaving deceased pensioners accounts in the system but changing recipients' bank account numbers. Auditors noticed unusual activity in March when pensioners must verify their existence.
1971 71314	Reiner von sur Muhlen, Wirtschaft und Politik, 10/10/71 computer manufacturer	No	Payroll theft	U.S. firm, victim	Apprehended	EDP operator pressed the "repeat" button on the printer to print 200 extra copies of his check. He was caught when he cashed 37 checks all at the same bank.
1971 71315	Reiner von sur Muhlen, Wirtschaft und Politik, 10/10/71 computer manufacturer Administrator of Natl. Banks, Office of the Controller of Currency, U.S. Treasury	No	Embezzlement $6.8 million	U.S. bank, victim	Apprehended	A vice president and employee of a discount chain credited incoming checks in the computer system but not the old parallel ledger system during changeover to the computer. The bank Vice President was promoted to a new job and had to erase evidence and was caught.

APPENDIX F (continued)

Case Data/Code	Source	Verified	Type	Principals	Disposition	Description
1971 71316	Reiner von sur Muhlen, Wirtschaft und Politik, 10/10/71 computer manufacturer British Assoc. for resocialization of ex-convicts	No	Embezzlement £17,000	British, firm, victim	Convicted. Served 2 years in prison	Programmer transferred £17,000 to a special error write-off account.
1971 71317	Reiner von sur Muhlen, Wirtschaft und Politik, 10/10/71	No	Embezzlement	A bank, victim		An accounting programmer changed a limit check for $2000 to $200,000 to claim a higher amount of credit than was allowed.
1971 71318	Reiner von sur Muhlen, Wirtschaft und Politik, 10/10/71 CPA Assistant who traced the manipulator	No	Embezzlement 480,000DM	Hamburg bank, victim		A programmer collected round-downs.
1971 71215	Reiner von sur Muhlen, Wirtschaft und Politik, 10/10/71 CPA Assistant who traced the manipulator	No	Data theft	U.S. economic data collection firm, victim	Employees fired	Two employees extracted and sold data. After they were fired, they tried to get others to do the same thing.

APPENDIX F (eoneluded)

Case Date/Code	Source	Verified	Type	Principals	Disposition	Description
1972 7246	Computer World 12/20/72, 1/31/73	No	Fraud $100,000	City of Honolulu Mayor Frank Fasi, victims; Larry E. Stevens, suspeet		An ex-analyst in the Dept. of Information Systems claimed the Mayor used city eomputer serviees for his reelection eampaign.
1973 7321	Computer World	No	Civil suit $25 million	IBM, plaintiff. Telex, Tulsa, Okla., defendant	Suit filed	IBM claims Telex engages in industiral espionage.
1969 6924	Commercial time-sharing staff 1/23/73	Yes	Fraud	Commereial time-sharing company, vietim; employee of another time-sharing eompany, perpetrator	Questionable ethies	A systems programmer gained legitimate LOGON to his employer's eompetitor's serviee and tested possible privileged system commands. He diseovered enough weaknesses to penetrate privileged mode where he could obtain eonfidential data.

Appendix G

CASE HISTORIES INVOLVING MULTIACCESS COMPUTER SYSTEMS

Appendix G

CASE HISTORIES INVOLVING MULTIACCESS COMPUTER SYSTEMS

NOTE

The purpose of this appendix is to assemble in one place references to cases involving unauthorized access to or other compromise of a time-sharing system. A common feature of many of these cases is the subversion or penetration of operating system security. Many of the cases mentioned in this appendix are described in somewhat greater detail in Appendix F.

Case No.	Case Name	Type of Threat	Description
6924	Tymshare System	Penetration of competitor's computer system from a terminal	Penetration started with trial and error discovery of privileged commands. Tymshare error messages helped to sort out legitimate commands. Penetration required about 1 1/2 months and about 40 hours of terminal time.
7042	Metridata Time-Sharing Penetration	Unauthorized terminal access to the operating system of a commercial time-sharing service	Involved a GE 400 time-sharing system. Access was made using known passwords and capture of a leased line. FORTRAN allowed execution of an assigned GO TO transferring control to user's COMMON area where data was executed that referenced an illegal address. This caused an interrupt, at which point the operating system was captured in master mode. System and user files were obtained and the system was crashed on numerous occasions.
7045	Illegal password usage	Accidental acquisition of unauthorized password	Two engineers accidentally discovered that a password one digit different from theirs allowed access to privileged customer and accounting data. Discovery was made when computer operators noticed use of password at unusual times.
7112	Metropolitan Life data net sabotage	Interruption to data communication network	By telephoning a tape recording of the signals used by a central computer to poll remote data stations, saboteurs managed to prevent the printout of processed data in about 25 branch offices.

Case No.	Case Name	Type of Threat	Description
7116	Stanford time sharing vandalism	Attempted modification of operating system	A student tried to erase every VTOC on each disk pack in the system. He succeeded in erasing only one, using a readily available IBM utility program. Use of that utility now requires a password.
7121	ISD vs UCC Program Theft	Theft of a program listing	An employee of UCC used a UCC remote job entry terminal and public telephone circuits to steal a listing of a program stored in the ISD computer and alleged to be a trade secret of ISD.
7128	Computer Sharing Services (CSS) vs Computer Time Corp (CTS)	Alleged software theft	Presently in litigation. Plaintiff (CSS) alleges that three former employees appropriated proprietary software (used in a GE-400 system) for the benefit of a competitor.
7221	Schneider/PT&T	Theft of equipment using computer-ordering codes	Schneider found various codes used in a PT&T equipment ordering system known as RAMAC and running on an IBM 360 in batch mode. Basic information was found in a company wastebasket. He formed a company to market equipment thus obtained. Was reported to police by an informer.
7228	University Computation Center November 1972	Password file theft	A student copied 5000 passwords from the system file by using a text editor. Password file is now kept in scrambled form.
72210	TRW Credit data theft	Unauthorized access to a confidential file	A former employee obtained credit reports by using the identification password of a legitimate subscriber to the service. The number was changed.

Case No.	Case Name	Type of Threat	Description
72214	Data theft from on-line system	Theft of confidential data	Dossiers taken from a large data bank system were being sold on the black market. System used a B6700. A specific dossier was flagged, an agent asked for this one through the black market, and the individual asking for this file from an on-line terminal was apprehended.
7244	High school student's unauthorized access to a national time-sharing service	Theft of time on a large system	Student found terminal output listings in a wastebasket. Had access to terminal through high school computer education program. Listings included account numbers and passwords. He proceeded to use large amounts of computer time. Discovered by an operator who noticed activity at unusual times.
7311	Dartmouth BASIC system Trojan Horse penetration	Entry gained into system as a challenge	A student's program checked privilege level. It could take over executive and invoke another privileged program that removed all evidence of penetration. The extra, privileged, program was discovered in a core dump.

Distribution

LLL Internal Distribution

R. P. Abbot (L-307) 300

TID Library 3

External Distribution

Mr. T. B. Barron
Senior E.D.P. Auditor
Great Western Financial Corp.
8484 Wilshire Blvd.
Beverly Hills, California 90211

Mr. Arthur Konopka
Social Systems
National Science Foundation
Washington, D.C. 20550

Mr. Robert H. Courtney, Jr.
IBM Corporation
P. O. Box 390
Dept. D05, Bldg. 707
Poughkeepsie, New York 12602

Mr. A. L. Tritter
T. J. Watson Research Center
Yorktown Heights, New York 10598

Mr. John G. Pierce
469 Massachusetts Avenue
Lexington, Massachusetts 02173

The Honorable Mike Cullen
Room 5144
State Capital
Sacramento, California 95814

Dr. Franklin H. Westervelt
Director
Computing and Data Processing Center
Wayne State University
Detroit, Michigan 48202

Major Roger R. Schell
Hq ESD (MCIT)
L. G. Hanscom Field
Stop 36
Bedford, Massachusetts 01730

Mr. Tom Bernard
Rohr Corporation
Chula Vista, California 92012

Verband Fur Sicherheit in der
Wirtschaft E. V.
43 Essen 1
Postfach 615/Fernruf: 22 71 47/48
Germany

Mr. H. von Seydlitz
Postbox 145
Eindhoven, Holland

Prof. Jerome Saltzer
Project MAC
545 Technology Square
MIT
Cambridge, Massachusetts 02139

Dr. John Weil
Honeywell Information Systems, Inc.
200 Smith Street
Waltham, Massachusetts 02154

Mr. T. M. Patton, Manager
Bond & Burglary Underwriting Dept.
Lumbermen's Mutual Casualty Company
Long Grove, Illinois 60049

Dr. H. S. Gellman
DCF Systems Limited
74 Victoria Street
Toronto 210, Ontario, Canada

Mr. George Hallock
International Data Security
1908 Windward Lane, Suite 100
Newport Beach, California 92660

Mr. Jerry Schneider
EDP Security, Inc.
1880 Century Park East
Suite 1000, Century City
Los Angeles, California 90067

External Distribution (Continued)

Mr. Gerald McKnight
3 Oakleigh Park Avenue
Chislehurst, Kent, England

Mr. Robert Morris
Control Data Corporation
8100 34th Avenue S.
Minneapolis, Minnesota 55420

Dr. Clair Miller
Singer Business Systems
San Leandro, California

Mr. James Matschulat
Risk Treatment Services Co.
6 E. 43rd Street
New York, New York 10017

Ms. Francis Furness
Editora Adril
11 W. 42nd Street
New York, New York 10036

Prof. Gideon Sjoberg
Dept. of Sociology
University of Texas at Austin
Austin, Texas 78712

Col. Phillip H. Enslow, Jr.
Office of Telecommunications Policy
Executive Office of the President
1800 G Street, N.W.
Washington, D. C. 20504

Mr. Robert Bigelow
Room 2200
28 State Street
Boston, Massachusetts 02109

Mr. F. M. Auburn
Lecturer in Law
The University of Auckland
Auckland, New Zealand

Mr. E. H. Clamons, Consultant
Honeywell Information Systems, Inc.
Deer Valley Park, P. O. Box 6000
Phoenix, Arizona 85005

Mr. B. J. Benzimra
Computuguard Ltd.
5 Penrhyn Rd.
Kingston upon Thames
Surrey, KT1 2BT
England

Prof. Allen H. Bizzell
Business-Economics Bldg. 300
University of Texas
Austin, Texas 78712

Prof. Ronald D. Jones
University of Missouri
School of Administration
Oxford Hall
Kansas City, Missouri 64110

Captain John C. Tardy
Dept. of the Army
Headquarters, U.S. Army Military
Police School
Fort Gordon, Georgia 30905

Mr. Norman Hardy, Director of
Technical Development
Tymshare Corp.
10231 Bubb Road
Cupertino, California 95014

Mr. Edgar C. Hayden
U.S. Dept. of Commerce
Institute for Telecommunication
Sciences
Boulder, Colorado 80302

Mr. Cameron Allen, Law Librarian
Rutgers University
Law School Library
180 University Avenue
Newark, New Jersey 07102

Herr Rainier A.H. von zur Mühlen
Von zur Mühlen'sche Unternehmens-
beratungsgesellschaft in BH
53 Bonn 1, Blücherstrasse 1A
West Germany

External Distribution (Continued)

Dr. Harold Sackman
The RAND Corporation
1700 Main Street
Santa Monica, California 90406

Mr. Ron Slivka
Operating Research Group
Morgan Guarantee Trust Co.
37 Wall Street
New York, New York 10015

Dr. Rein Turn
The RAND Corporation
1700 Main Street
Santa Monica, California 90406

Dr. Richard Mills
First National City Bank
399 Park Avenue, Tube 33
New York, New York 10022

Mr. Richard Webb
Touche Ross & Co.
1633 Broadway
New York, New York 10019

Ms. Elsie Lee
Honeywell Information Systems, Inc.
1 Maritime Plaza
Suite 960
San Francisco, California 94111

Mr. James Anderson
P. O. Box 42
Fort Washington, Pennsylvania 19034

Mr. Kenneth Orr, Chairman
NASIS Committee on Privacy,
Confidentiality & Security
Data Processing Services
Dept. of Administration
State of Kansas
Statehouse
Topeka, Kansas 66612

Mr. Peter Hamilton
44 Chancery Lane
London, W.C. 2, England

Mr. Thomas Wolf
Wirtschaftspublizistik
Kilchbergsteig 11
8038 Zurich, Switzerland

Dr. Peter J. Lykos
National Science Foundation
Office of Computing Activities
Washington, D.C. 20550

Mr. Jerry Kennedy
Basic Computing Arts
3197 Park Blvd.
Palo Alto, California 94304

Dr. Ruth M. Davis
Institute for Computer
Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234

Mr. Robert S. Fabry
Computer System Research Project
2000 Center Street, Suite 301
Berkeley, California 94704

R. Stockton Gaines
Institute for Defense Analyses
100 Prospect Avenue
Princeton, New Jersey 08540

Dr. Lance J. Hoffman
Dept. of EE & CS
University of California
Berkeley, California 94720

Dr. Eldred C. Nelson
TRW Systems Group
One Space Park
Redondo Beach, California 90278

Dr. Robert H. Scott
Massachusetts Institute of Technology
39-565
77 Massachusetts Avenue
Cambridge, Massachusetts 02115

External Distribution (Continued)

Mr. Clark Weissman
Systems Development Corporation
2500 Colorado Blvd.
Santa Monica, California 90406

Dr. Theodore Linden
National Security Agency
R52
Fort George G. Meade, Maryland 20755

Mr. Quon Y. Kwan
Bldg. 130, Room 755
The Aerospace Corp.
P. O. Box 95085
Los Angeles, California 90045

Mr. Oliver R. Smoot, Director of
Industry Programs
Computer and Business Equipment
Manufacturers Association (CBEMA)
1828 L Street, N.W.
Washington, D.C. 20036

Mr. Thomas E. Schatzel
Suite 104
1333 Lawrence Expressway
Santa Clara, California 95051

Mr. Edgar C. Hayden
Institute for
Telecommunications Sciences
Boulder, Colorado 80302

Mr. Roy N. Freed
Widett & Widett
One Federal Street
Boston, Massachusetts 02110

Mr. Vico Henriques
CBEMA
1828 L Street N.W.
Washington, D.C. 20036

Mr. William Hanna, Jr.
Room 302
Social Security Administration
Baltimore, Maryland 21235

Mr. Milton Wessel
Kaye, Scholer, Fierman, Hays & Handler
425 Park Avenue
New York, New York 10022

Mr. George E. Goode
Datatek
8220 Westchester
Dallas, Texas 75225

Mr. Gerald Van Dorn
Chase Manhattan Bank
1 Chase Manhattan Plaza
New York, New York 10015

Mr. Sumio Ishizaki
The Fuji Bank
1-Chome, Otemachi
Chiyoda-Ku
Tokyo, Japan

Mr. Fred Tippett
American Bankers Association
1120 Connecticut Ave., N.W.
Washington, D.C. 20036

Mr. Robert Jacobson
Sentor Security Group
17 Battery Place
New York, New York 10004

Mr. Jerome Lobel
Dataguard Systems
700 W. Campbell Avenue
Phoenix, Arizona 85013

Mr. Jack Bremer
Honeywell Information Systems, Inc.
P. O. Box 6000
Phenix, Arizona 85005

Mr. Charles C. Marson
ACLU Foundation of Northern California
593 Market Street, Suite 227
San Francisco, California 94105

Dr. G.B.F. Niblett
14 Fitzharry's Road
Abington, Berkshire
England

External Distribution (Continued)

Mr. Robert P. Henderson
Honeywell Information Systems, Inc.
200 Smith Street
Waltham, Massachusetts 02154

Prof. Michael Duggan
BEB-608
University of Texas
Austin, Texas 78712

Dr. Robert R. J. Gallati
New York State Identification System
Executive Park Tower
Stuyvesant Plaza
Albany, New York 12203

Prof. Donald R. Cressey
Ellison Hall
University of California
Goleta, California 93017

Prof. John Kaplan
Room 215
Stanford School of Law
Stanford, California 94305

Mrs. Susan Nycum
Room 4
Stanford School of Law
Stanford, California 94305

Mr. Victor T. Esposito
Chief Special Agent
Pacific Telephone and Telegraph Co.
742 S. Hill Street
Room 200
Los Angeles, California 90014

Dr. Robert Wong
Dept. of Savings & Loan
State of California
3440 Wilshire Blvd.
Los Angeles, California 90010

Mr. Robert T. Caravella
Project Manager, Secure Automated Facility Environment (SAFE) Project
State of Illinois
Department of Finance (MID)
604 State Office Building
Springfield, Illinois 62706

Mr. Theodore Eldlin
NASA Ames Research Center
Moffett Field,
Sunnyvale, California 94086

Dr. Melvin Pirtle
NASA Ames Research Center
Moffett Field
Sunnyvale, California 94086

Mr. Richard Bisbey
ISI
4676 Admiralty Way
Marina Del Rey, California 90291

Mr. Steve Crocker
Advanced Research Projects Agency
1400 Wilson Blvd.
Rosslyn, Virginia 22206

Mr. Rod Fredricksen
The RAND Corporation
1700 Main Street
Santa Monica, California 90406

Mr. Julius Debro
Institute of Criminal Justice and Criminology
College of Arts and Sciences
University of Maryland
College Park, Maryland 20742

Mr. Darryl Fine
EDP Audit Department
Wells Fargo Bank
44 Montgomery Street
4th Floor
San Francisco, California 94104

External Distribution (Continued)

Mr. Dick Mills
EDP Security
First National City Bank
New York, New York

Professor James D. Calder
University of Maryland
Institute of Criminal Justice
and Criminology
College of Arts and Sciences
College Park, Maryland 20742

Mr. Steven B. Lipner
Subdepartment Head
Management and Computer Systems
The Mitre Corporation
Bedford, Massachusetts 01730

Professor Herbert B. Baskin
Director, Computer Systems
Research Project
University of California
2000 Center Street
Berkeley, California 94720

Mr. George T. Steeley, Jr.
President, Information Systems
Design
7817 Oakport Drive
Oakland, California 94621

Mr. William Bennett
Comshare
3853 Research Drive
Ann Arbor, Michigan 48103

Mr. Arthur Evans, Jr.
Lincoln Labs
P. O. Box 73
Lexington, Massachusetts 02173

Mr. Virgil H. Disney
Director Research Division
Bank Administration Institute
303 S. Northwest Highway
Park Ridge, Illinois 60068

Mr. Noel K. Zakin
Manager, Computer Technical Services
American Institute of Certified
Public Accountants
666 Fifth Avenue
New York, New York 10019

Mr. Roy Crystal
Evaluation Branch, CHS
5600 Fishers Lane
Rockville, Maryland 20852

Mr. Harvey W. Bingham
Manager Product Security
P. O. Box 203
Paoli, Pennsylvania 19301

Mr. Lee Danner
Systems Development Division
18100 Frederick Pike
Gaithersburg, Maryland 20760

Mr. Dan Bertram
Tinley Park Mental Health Center
Information Systems, Subregion 14
7400 West 183rd Street
Tinley Park, Illinois 60477

Mr. James M. Clayton
ODASD (Security Policy)
OASD, Comptroller
Room 3C 283 Pentagon
Washington, D.C. 20301

Dr. Ronald Finkler
Institute of Defense Analysis
Science and Technology Division
400 Army-Navy Drive
Arlington, Virginia 22202

Captain Fuk W. Leong
AFDSC/XM
Washington, D.C. 20330

Mr. Jerry Short
TRW Systems
One Space Park
Redondo Beach, California 90278

External Distribution (Continued)

Mr. Marvin Lesser
McKinsey and Company
245 Park Avenue
New York, New York 10017

Mr. Tim Braithwaite
DOD Computer Institute
Building 175
Washington Navy Yard
Washington, D.C. 20390

Commander
Joint Technical Support Agency
Attention: Code J410 (Mr. Inglis)
1860 Wiehle Avenue
Reston, Virginia 22090

Mr. A. L. Schulte
McDonnell Douglas Automation Co.
P. O. Box 516
St. Louis, Missouri 63166

Computer Center Library, FC-10
University of Washington
Seattle, Washington 98195
Attn: Ms. Darlene Myers
Librarian

T.I.C. Oak Ridge 2

IMM/js

☆ GPO 791-022